Tony Myllylä

Sähköverkkojen kyberturvallisuus

Sähkötekniikan korkeakoulu

Diplomityö, joka on jätetty opinnäytteenä tarkastettavaksi
diplomi-insinöörin tutkintoa varten Espoossa 27.1.2014.

Työn valvoja:

Prof. Matti Lehtonen

Työn ohjaaja:

Prof. Matti Lehtonen

Aalto-yliopisto
Sähkötekniikan
korkeakoulu

AALTO-YLIOPISTO DIPLOMITYÖN TIIVISTELMÄ
SÄHKÖTEKNIIKAN KORKEAKOULU

Tekijä: Tony Myllylä
Työn nimi: Sähköverkkojen kyberturvallisuus
Päivämäärä: 27.1.2014 Kieli: Suomi Sivumäärä: 62
Sähkötekniikan ja automaation laitos
Professuuri: Sähköverkot ja suurjännitetekniikka
Koodi: S-18
Valvoja: Prof. Matti Lehtonen
Ohjaaja: Prof. Matti Lehtonen

Tässä työssä tarkastellaan sähköverkkojen kyberturvallisuutta. Kyber-sanan käyttö on lisääntynyt merkittävästi kasvaneen tietoverkkorikollisuuden myötä. Tiedon siirtyminen verkkoon on lisännyt haasteita tietoturvan suhteen myös teollisuusautomaatiolaitteissa. Sähköverkot ovat infrastruktuurimme tärkein tukipilari, joten niiden suojaaminen kyberhyökkäyksiltä on ensisijaisen tärkeää.

Nykyaikainen sähkönsiirto on pitkälti automatisoitunutta. Sitä valvotaan ja ohjataan keskitetysti valvomoista, joissa käytönvalvonta- ja käytöntukijärjestelmällä on erittäin tärkeä rooli. Niiden avulla kyetään ohjaamaan ja hallitsemaan koko valtakunnan sähköverkkoa. Käytönvalvontajärjestelmä (SCADA) on erittäin haavoittuvainen erilaisille tietoverkoissa piileville haittaohjelmille, joilla on kyky lamaannuttaa koko järjestelmä.

Työn alussa tarkasteltiin teoreettisella tasolla sähkönsiirto- ja jakeluverkon toimintaa ja niissä käytettyjä automaatio- ja tiedonsiirtojärjestelmiä. Lisäksi tutustuttiin erilaisiin tiedonsiirtoprotokolliin ja tietokantoihin. Lopussa keskityttiin erilaisiin kyberturvallisuusuhkiin, niiltä suojautumiseen sekä kansainvälisesti tunnettuihin kyberhyökkäyksissä käytettyihin haittaohjelmiin.

Kyberrikollisuuden kasvun myötä myös maan poliittinen johto on ottanut asian tarkastelun alle ja luonut oman kyberturvallisuusstrategiansa uhkakuvien torjumiseksi. Tämän strategian käsittely on osana tätä työtä.

Avainsanat: Käytönvalvontajärjestelmä, Käytöntukijärjestelmä, Kyber-, haittaohjelma, tiedonsiirtoprotokolla.

AALTO UNIVERSITY
THE SCHOOL OF ELECTRICAL ENGINEERING
THESIS

ABSTRACT OF MASTER'S

Author: Tony Myllylä
Title: The Electric grid´s cyber security.
Date: 27.1.2014 Language: Finnish Number of Pages: 62
Department of Electrical Engineering and Automation
Professorship: Power Systems and High Voltage Engineering
Code: S-18
Supervisor: Prof. Matti Lehtonen
Instructor: Prof. Matti Lehtonen

This diploma thesis discusses the cyber security of an electric grid. Use of Cyber word has grown significantly due to increased cybercrime. The increased amount of information on the network has increased the challenge of cyber security on the industrial automation devices. Electric grids are the key component of the infrastructure, so the protection of cyber attacks is a top priority.

Modern electric transmission is largely automated. It is monitored and controlled from centralized control stations, where the use of the Supervisory Control and Data Acquisition and Distribution Management Systems have a significant role. These systems control and adjust the different levels and parts of the national electric grid. Supervisory Control and Data Acquisition System (SCADA) is highly vulnerable to different types of malware with the ability to paralyze the entire system.

The first part of this diploma thesis discusses the theoretical level of power distribution system operation and related automation and communication systems. In addition, communication protocols and databases are presented. The second part of this diploma thesis focuses on different types of cyber security threats. Commonly known malware is presented and methodology how to protect the systems from cyber-attacks is discussed.

Concerning the increased amount of cybercrime, the Finland´s political leaders have taken this issue seriously, and cyber security strategy has been created to combat this threat. The discussion of this strategy is part of this work.

Keywords: Supervisory Control and Data Acquisition system, Distribution Management System, Cyber,-malware, communication protocol.

Esipuhe

Tämä diplomityö käsittelee sähköverkkojen kyberturvallisuutta ja on tehty opinnäytteeksi Aalto- yliopiston Sähkötekniikan korkeakoulun Sähkötekniikan ja automaation laitokselle. Työlle on ollut tilausta sillä kyberhyökkäykset ovat lisääntyneet merkittävästi viime vuosina ja aiheuttaneet suuria taloudellisia vahinkoja infrastruktuurin eri osa- alueilla. Erityisesti sähköverkkojen haavoittuvuus kyberiskulle on ollut tiedossa mutta sen lähempi tarkastelu on jäänyt huomioimatta.

Haluan esittää kiitokset työn valvojalle ja ohjaajalle professori Matti Lehtoselle, joka taustani huomioiden, esitti tätä mielenkiintoista ja ajankohtaista työtä minulle, antaen laajan liikkumavaran sen toteuttamiselle.

Lisäksi kiitän kaikkia niitä asiantuntijoita, joiden kanssa olen käynyt henkilökohtaisia keskusteluja aiheesta. Heidän arvokkaat neuvot ja ohjeet ovat suuresti helpottaneet kirjoitustyötäni ja ymmärrystäni asiassa.

Lämpimät kiitokset myös lähipiirilleni, jotka ovat tukeneet minua tässä pitkässä opiskeluprojektissa.

Kirkkonummella 27.1.2014

Tony Myllylä

SISÄLLYSLUETTELO

Käytetyt lyhenteet

2G	*2nd Generation,* Toisen sukupolven matkapuhelinverkko.
3G	*3rd Generation,* Kolmannen sukupolven matkapuhelinverkko.
DA	*Distribution Automation,* Sähkönjakeluautomaatio.
KVJ	Käytönvalvontajärjestelmä.
SCADA	*Supervisory Control And data Acquisition,* Käytönvalvontajärjestelmä.
KTJ	Käytöntukijärjestelmä.
DMS	*Distribution Management System*, Käytöntukijärjestelmä.
GSM	*Global System for Mobile Communications*, Toisen sukupolven matkapuhelinjärjestelmä.
GPRS	*General Packet Radio Service*, Matkapuhelinverkon pakettikytkentäinen tiedonsiirtopalvelu.
TETRA	*Terestrial Trunked Radio*, Digitaalinen puheradioverkko.
UMTS	*Universal Mobile Telecommunication System*, Kolmannen sukupolven matkaviestinjärjestelmä.
PLC	*Power Line Communication*, Sähköverkkotiedonsiirto.
SMS	*Short Message Service*, matkapuhelimen tekstiviestijärjestelmä.
WCDMA	*Wideband Code Division Multiple Access*, Määrittelee mobiililaitteiden kommunikointitavan tukiasemien kanssa**.**
VPN	*Virtual Private Network*, Loogisesti erotettu suojattu verkko- osa.
TCP/ IP	*Transmission Control Protocol/ Internet Protocol*, Internet-pohjaiseen tiedonsiirtoon kehitetty protokolla.
ELCOM	*Electricity Utilities Communications*, sähkölaitosten valvomoiden väliseen energiatietojen siirtoon käytetty protokolla.
ICCP	*Inter- Control Center Communications Protokol*, Käytönvalvontajärjestelmien väliseen liikennöintiin tarkoitettu protokolla.
OSI	*Open Systems Interconnection*, Seitsemän kerroksinen tiedonsiirtostandardiperhe.
IEC 60870	IEC:n määrittelemä lähiverkkoprotokolla.

IEC	*International Electrotechnical Commission*, Sähköalan standardointijärjestö.
DNP3	*Distributed Network Protocol,* Käytönvalvontajärjestelmissä käytetty tiedonsiirtoprotokolla.
IED	*Intelligent Electronic Device*, Ohjelmoita elektroninen laite.
RTU	*Remote Terminal Unit*, Käytönvalvontajärjestelmän ala- asema.
MODBUS	Sarjaliikenneprotokolla, jota käytettään ohjelmoitavien logiikkapiirien kanssa.
PLC	*Programmable Logic Controller*, Ohjelmoitava logiikka.
ASCII	*American Standard Code for Information Interchange*, Tietokoneiden merkkijärjestelmä.
DSiP	*Distributed Systems Intercommunicaton Protocol,* Tiedonsiirtoa monikanavareititinympäristössä.
AMR	*Automatic Meter Reading*, Automaattinen mittarinluenta.
AMI	*Advance Metering Infrastructure,* Älykäs mittarointi.
DoS	*Denial- of- Service*, Palvelunestohyökkäys.
LAN	*Local Area Network,* Lähiverkko.
WAN	*Wide Area network*, Etäverkko.
IEEE	*Institute of Electrical and Electronic Engineers*, Sähköalan standardointijärjestö
NIST	*National Institute of Standards and technology*, Sähköalan standardointijärjestö.
NERC	*North American Electric Reliability Corporation*, Sähköalan järjestö.
CPNI	*Centre for Protection on National Infrastructure*, Sähköalan standardointijärjestö.
ETHERNET	Lähiverkoissa käytettävä tiedonsiirtomenettely.
IDS	*Intrusion Detection System*, Hyökkäyksen ja tunkeutumisen havainnointijärjestelmä.
IPS	*Intrusion Protection System*, Hyökkäyksen ja tunkeutumisen estojärjestelmä.

1. Johdanto

Nykyaikainen sähköntuotanto, -siirto- ja -jakelu on pitkälti automatisoitunutta ja tietojärjestelmäriippuvaista. Verkon laitteiston perinteinen valvontatapa on muuttunut fyysisen maailman ilmiöistä digitaalisen maailman ilmiöihin, jossa erilaisilla tietojärjestelmillä on merkittävä rooli. Tällaisia järjestelmiä ovat käytönvalvontajärjestelmä, käytöntukijärjestelmä, asiakastietojärjestelmä, tiedonsiirtojärjestelmä sekä verkkotietojärjestelmä. Näiden järjestelmien avulla, kyetään keskitetysti ohjaamaan ja valvomaan energian tuotanto- ja siirtoprosesseja. Sähkönjakeluautomaatio ja siihen kiinnitetyt tietojärjestelmät, asettavat tiukkoja tietoturvahaasteita verkon ylläpitäjille.

Organisoidulla ja arvaamattomalla kyberhyökkäyksellä kyetään lamaannuttamaan tietojärjestelmäpohjainen sähkönjakelujärjestelmä täysin. Tällainen kokonaisvaltainen sähköverkkoihin kohdistuva kyberhyökkäys kaataisi koko infrastruktuurijärjestelmämme. Hyökkäyksen rajapintana toimisi Internet ja infrastruktuurin ulkoiset rakenteet.

Valtioneuvosto on osaltaan ollut vaikuttamassa kyberturvallisuuteen, julkaisemalla 24.1.2013 oman kyberturvallisuusstrategiansa. Se pureutuu kyberrikollisuuden uhkakuviin ja ohjeistaa eri viranomaisia toimimaan yhteistyössä. Suomen kyberturvallisuuden periaatepäätös on osoitus siitä, että Suomi haluaa osaltaan olla estämässä kyberrikollisuuden leviämistä ja taata toimivan yhteiskuntaturvallisuuden sen kriittisillä osa- alueilla, kuten energian – ja sähkön jakelussa. Kriittisesti tärkeitä infrastruktuurin osa-alueita, kuten energiantuotantoa, sähkön-, öljyn- ja kaasun jakeluverkkoja on kyettävä puolustamaan myös virtuaalisessa maailmassa.

Tässä diplomityössä paneudutaan sähköverkkojen kyberturvallisuuteen ja tarkastellaan kyberturvallisuutta yleisesti. Käsitellään sähköverkon haavoittuvuutta kyberhyökkäykselle ja keinoja niiltä suojautumiseen.

Teknisen tietoturvan lisäksi työssä tarkastellaan nykyaikaisen sähköverkon rakennetta; sähkönjakeluverkon käyttötoimintaa, sähkönjakeluautomaatiota ja erityisesti sen käytönvalvontajärjestelmää sekä muita apuvälineitä, kuten tiedonsiirtomenetelmiä ja etäluettavia sähkömittareita.

Sähköverkkojen hallinta muodostuu verkon käytöstä, sen kunnossapidosta sekä kehittämissuunnittelusta, joista tässä käsitellään lähinnä verkon käyttöä. Lisäksi esitetään muutamia tunnetuimpia kyberhyökkäyksiä, niissä käytettyjä haittaohjelmia ja niiden toimintatapoja. Lopuksi tehdään yhteenveto sähköverkkojen haavoittuvuudesta, niiden suojauksesta ja muodostetaan kokonaiskuva Suomen tilanteesta.

Diplomityö perustuu pitkälti kirjallisuusselvitykseen, jonka tietoaines on kerätty alan julkaisuista. Työssä on lisäksi hyödynnetty asiantuntijahaastatteluja, jotka ovat tuoneet oman panoksensa niin suullisessa kuin kirjallisessakin muodossa. Asiantuntijat ovat tarkasti valikoituja ja pitkään sähköalalla työskennelleitä henkilöitä. He ovat omalta osaltaan olleet kehittämässä sähköverkkojen luotettavuutta ja tuntevat nykypäivän sähköverkkoihin kohdistuvat kyberuhat. Haastattelut ovat liitteenä.

2. SÄHKÖVERKKO JA TIETOJÄRJESTELMÄT

Sähkönsiirto- ja jakeluverkon käyttötoiminnassa hyödynnetään teollisuuden automaatiojärjestelmiä, joiden tehtävä on vähentää ihmisen tekemiä ohjauskäskyjä. Automaatiojärjestelmä koostuu erilaisista tietojärjestelmistä, joiden avulla kyetään ohjaamaan, seuraamaan ja hallitsemaan sähkön tuotanto- ja siirtoprosessia tarkasti ja luotettavasti [1].

Tässä luvussa käydään läpi sähköverkon rakennetta ja sen käyttöä. Tarkastellaan sähköteollisuudessa yleisesti käytössä olevia tietojärjestelmiä, käytönvalvontajärjestelmää ja käytöntukijärjestelmää, jotka ovat käyttötoiminnan kannalta tärkeimpiä. Lisäksi käsitellään eri järjestelmien välistä tiedonsiirtoa.

2.1 Sähkönjakeluverkon käyttötoiminta

Sähkönjakeluverkon käyttötoiminta tarkoittaa verkon käytönaikaista valvontaa ja ohjausta. Käyttötoiminnan tehtäviin kuuluu erilaisten häiriötilanteiden hallinta, käyttötoimintojen suunnittelu sekä verkon tilan seuranta. Toimintojen ohjaus tapahtuu kiinteästi valvomosta tai vaihtoehtoisesti käyttöpäivystäjän sijaintipaikasta tietoteknisiä apuvälineitä hyödyntäen, kuten Internetiä [2].

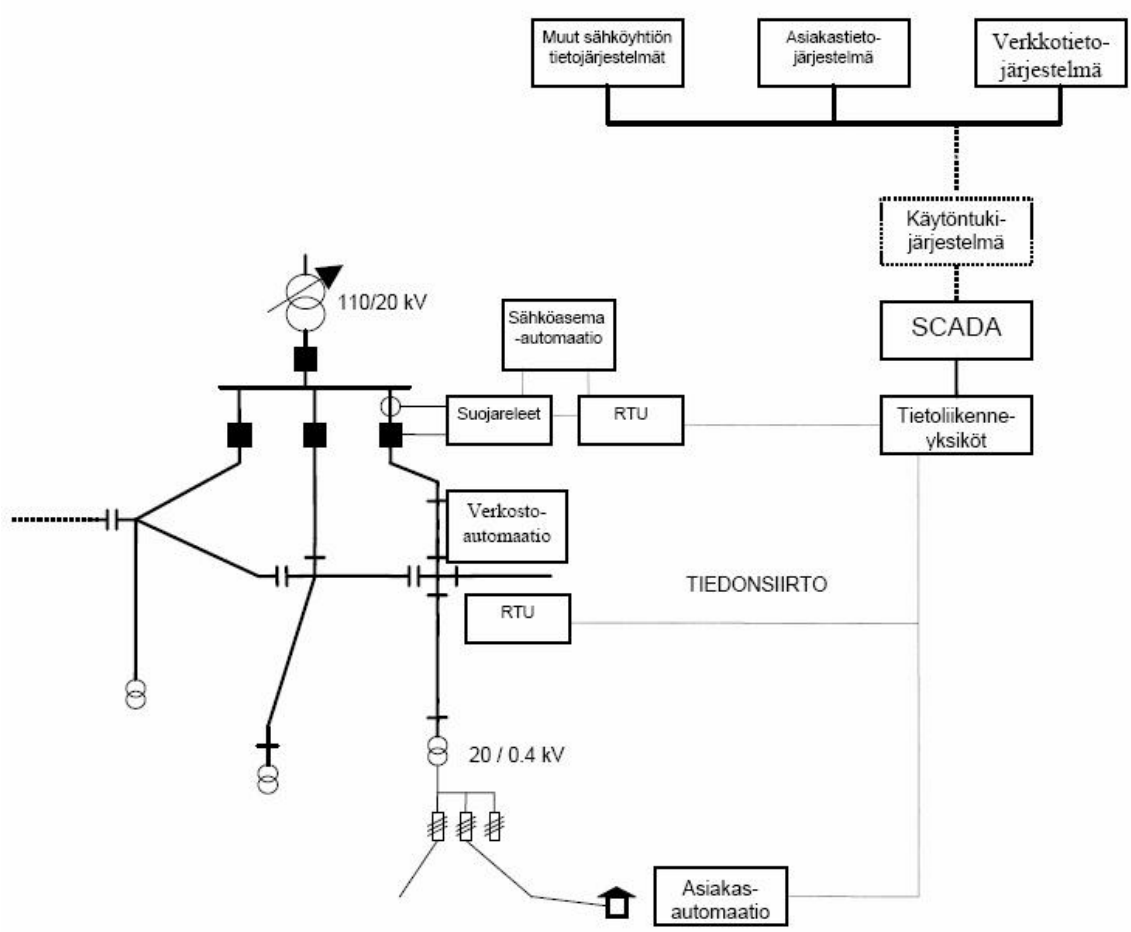
2.1.1 Sähkönjakelujärjestelmä

Sähkönjakelujärjestelmä kostuu kahdesta erillisestä järjestelmästä, primääri- ja sekundäärijärjestelmästä, joista jälkimmäisestä käytetään myös nimitystä sähkönjakeluautomaatio. Primäärijärjestelmällä tarkoitetaan sähkönjakeluverkkoa, johon sisältyy alue-, keski- ja pienjänniteverkot, sähköasemat ja jakelumuuntamot.

Sekundäärijärjestelmä koostuu tietojärjestelmistä, sähköasemien suojareleistä, verkon vianilmaisimista ja mittareista, kuten etäluettavista energiamittareista. Näiden lisäksi järjestelmään kuuluu käytönvalvonta- ja käytöntukijärjestelmät sekä muut tiedonsiirtojärjestelmät [2].

2.1.2 Sähkönjakeluautomaatio

Sähkönjakeluautomaatio (Distribution Automation, DA) muodostuu hierarkkisesta rakenteesta, jossa eri automaation osa- alueilla on oma niille säädetty tehtävä. Sähkönjakeluautomaation tasoja on esitelty kuvassa 1. [2].



Kuva 1. Verkon käyttötoiminnan apuvälineet [2].

Sähköverkon toiminnallisuus ja käytettävyys on kuvassa olevien apuvälineiden varassa. Näistä tärkeimpiä ovat suojareleet, käytöntukijärjestelmä sekä käytönvalvontajärjestelmät ja niiden väliset tiedonsiirtoväylät. Sähkönjakeluautomaatio jakaantuu viiteen automaatiotasoon. Tasot ovat kuvan 1. mukaisesti asiakas-, sähköasema-, verkosto-, valvomo ja yhtiöautomaatio.

Kaikilla näillä tasoilla on omat tiedonsiirron luotettavuus- ja aikakriittisyysvaatimukset. Automaatiotasojen välinen tietojenvaihto tapahtuu pääsääntöisesti radiolinkkiyhteyksin sekä sähköverkkotiedonsiirtona [2].

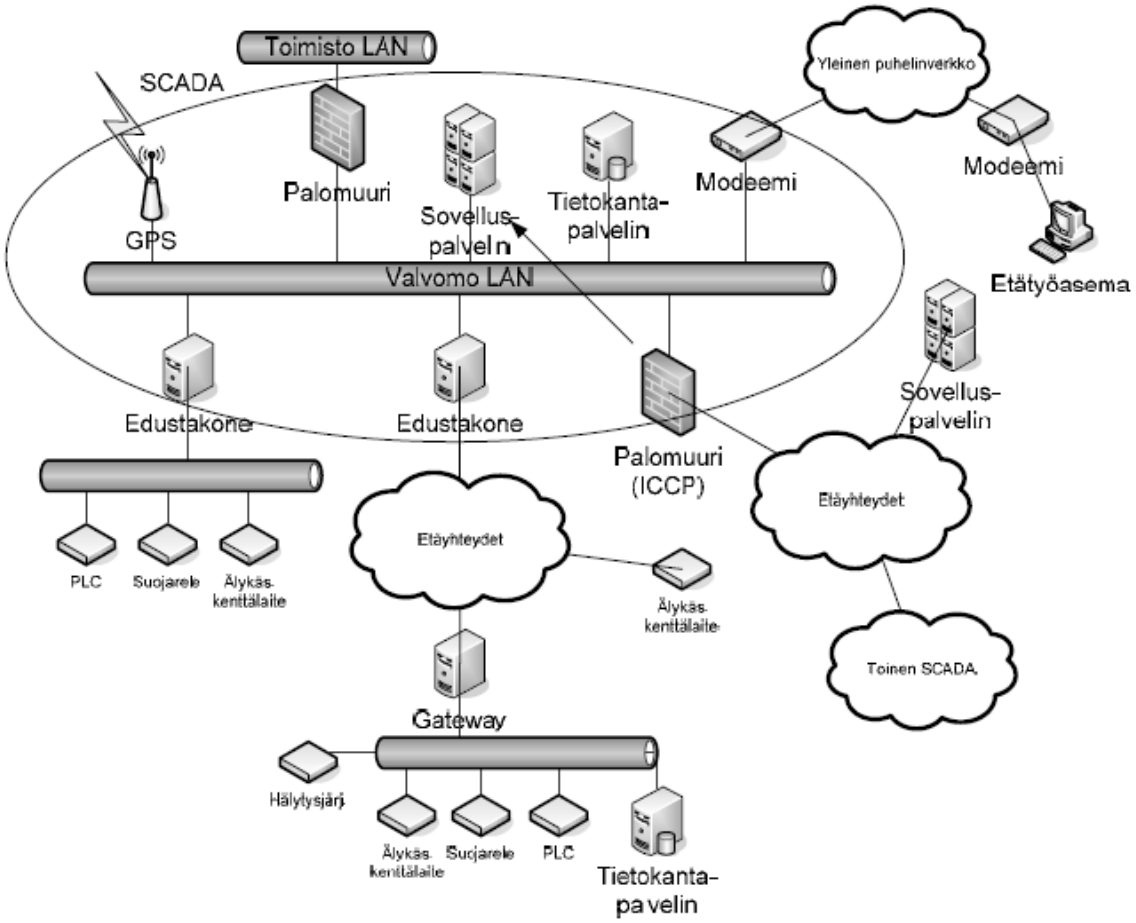
Kaikki edellä kuvatut sähkönjakeluautomaation tasot ja niiden väliset tiedonsiirtotekniikat ovat potentiaalisia verkkohyökkäyksen kohteita.

2.2 Käytönvalvontajärjestelmä

Sähköverkon reaaliaikaisesta valvonnasta ja tietojenkeruusta vastaa käytönvalvontajärjestelmä (KVJ). Kansainvälinen nimitys tälle järjestelmälle on SCADA (Supervisory Control and Data Acquisition). Tämä teollisuudessa yleisesti käytössä oleva automaatiojärjestelmä välittää mittaus-, tila- ja tapahtumatietoja voimajärjestelmän tilasta. Sen avulla kyetään ohjaamaan verkon katkaisijoita ja erottimia sekä hallinnoimaan erilaisia kytkentätilanteita. Järjestelmän avulla kyetään lisäksi muodostamaan reaaliaikainen yhteys sähköasemiin ja muihin kriittisesti tärkeisiin kohteisiin [2, 3, 4].

Käytönvalvontajärjestelmän toimivuus on ensisijaisen tärkeää, mistä johtuen SCADA-järjestelmässä kiinni olevat palvelimet, reitittimet ja tietoliikenneyhteydet ovat ns. ”kuumakytkettyjä” eli kaksoisvarmennettuja siten, että laitteen vikaantuessa, varalaite ottaa järjestelmän tehtävät haltuunsa niin, ettei verkon tilatiedot pääse katoamaan ja järjestelmän toimivuus säilyy ennallaan. Tietokanta ja käyttöliittymä, joihin käytönvalvontajärjestelmä perustuu, pitää sisällään tarkat tiedot sähköasemista ja niiden laitteistosta. Mittaus- ja tilatietojen, kuten kuormitus- ja vikavirtojen sekä generaattoritehojen lisäksi, järjestelmä viestii kytkinlaitteiden asentotiedot [2, 3].

Nykyaikaista käytönvalvontajärjestelmää ja sen laitteistokokoonpanoa on esitelty kuvassa 2.



Kuva 2. Käytönvalvontajärjestelmän arkkitehtuuri [5].

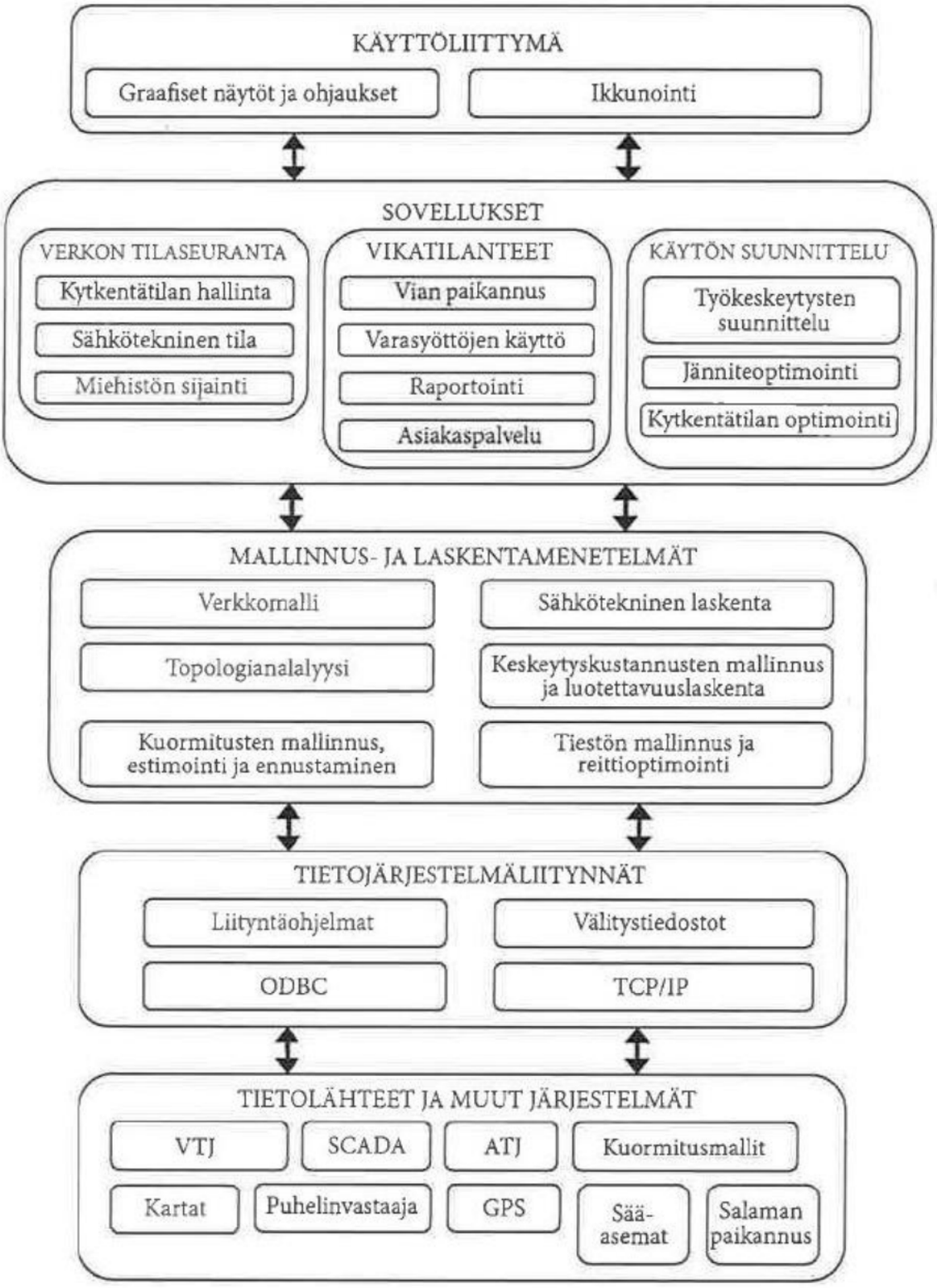
SCADA- järjestelmä koostuu monista eri komponenteista. Kaikkien kuvassa esiintyvien käyttöalueiden tiedot ovat yhteiskäytössä ja niitä pystytään muokkaamaan erilaisilla ohjelmistoilla, jotka helpottavat valvontajärjestelmän käyttötoimintaa. Järjestelmän muita pääkomponentteja ovat palvelimet, reitittimet, varavalvomo sekä tietoliikenneyhteydet [4].

2.3 Käytöntukijärjestelmä

Käytöntukijärjestelmä (KTJ) toimii älykkäänä päätöksenteon työkaluna verkon käytöstä vastaavien henkilöiden tukijärjestelmänä. Kansainvälinen nimitys järjestelmälle on DMS (Distribution Management System). Toiminnaltaan se eroaa SCADA- järjestelmästä ”älyssä”. DMS sisältää enemmän analyysi- ja päättelytoimintoja, joissa se hyödyntää eri tietojärjestelmiä.

Käytöntukijärjestelmä edellyttää kuitenkin SCADA- järjestelmän rinnalla oloa, jotta se saa tarvittavaa tietoa prosesseista ja kykenee ohjaamaan niiden toimintaa [2].

Käytöntukijärjestelmän sisältämä ohjelmisto on monipuolinen ja se sisältää hyvin monia toimintoja ja liityntöjä muihin tietojärjestelmiin. KTJ jakaantuu viiteen eri tasoon, jotka on esitetty kuvassa 3.



Kuva 3. Käytöntukijärjestelmän tasot ja liitynnät [2].

Tällaisessa laaja- alaisessa informaation hyödyntämisessä piilee omat vaaransa, sillä ne lisäävät sähköyhtiöille paineita tietoverkkojen laajamittaisempaan käyttöön. Ongelmana on, että sovelluskohtaisten standardien ja ohjeiden puuttuessa tietoturvariskit lisääntyvät. Tietoturvaa käsitellään yksityiskohtaisemmin luvussa 6.

3. Sähköverkon tietoliikenne ja protokollat

3.1 Sähköverkon tiedonsiirto

Sähköverkkoyhtiöiden tietojärjestelmät hyödyntävät jatkuvasti monista lähteistä saatavaa tietoa. Osalle tiedonsiirrosta asetetaan luotettavuus- ja aikakriittisyysvaatimuksia. Osa järjestelmistä on välittömässä yhteydessä kenttälaitteisiin, osan välittäessä tietoja aikaviiveellä. Aikakriittisyys on valvomon ja sähköaseman välisessä tietojen vaihdossa erityisen tärkeää, kun taas valvomon ja verkon välinen tiedonsiirto vähemmän aikakriittistä. Tiedonsiirtotekniikoilla on tässä prosessissa erityisen tärkeä merkitys. Yleisesti käytössä olevia tiedonsiirtotekniikoita ovat [2]:

- valokuitu
- radiolinkkiyhteys
- kiinteä kaapeli
- GSM, GPRS
- radiopuhelinverkko (TETRA)
- satelliitti
- matkapuhelinverkot 2G, 3G
- sähköverkkotiedonsiirto (PLC, Power Line Communication)

Edellä kuvatuista tiedonsiirtomenetelmistä, yleisimpiä Suomessa käytössä olevia ratkaisuja ovat kaapeli- ja radiolinkkiverkot. Edellä kuvattujen tekniikoiden valinnassa vaikuttaa viestiyhteyksien käytettävyys sekä kustannustehokkuus [4].

Kaapeloinnin hyviä puolia on sen taloudellisuus lyhyillä viestiyhteyksillä kun taas pitkillä etäisyyksillä tiedonsiirtoa rajoittaa erilaiset vääristymät. Radiolinkkien käyttö on taloudellista pitkillä viestiyhteyksillä, ala- ja keskusaseman välisessä tiedonsiirrossa.

Radiopuhelinyhteydet ovat yleistyneet verkkoyhtiöiden tiedonsiirrossa. TETRA-verkko (Terrestrial Trunked Radio) on viranomaisten käyttöön tarkoitettu matkapuhelinverkko, joka tukee puhe- ja tiedonsiirtoa.

TETRA- verkon käyttöä tiedonsiirrossa tukee sen salausjärjestelmä, josta käytettään nimeä ilmarajapintasalaus. Sen avulla kyetään salaamaan tukiaseman ja päätelaiteen välinen liikenne. Radiopuhelinyhteydet hyödyntävät vapaita taajuuksia, joiden käyttö on ilmaista. Tällaisia ilmaiskanavia käytetään muun muassa energiamittareiden kaukoluennassa [4].

Matkapuhelinratkaisuja on otettu käyttöön alueilla, jotka ovat hyvin laajoja. Puhelinverkkojen luotettavuudesta huolimatta, niiden käyttö automaatiossa on rajoittunutta. Matkapuhelinverkot ovat suorituskyvyltään niin suuria, että niissä voidaan käyttää useampia eri toimintoja samassa palvelussa. Tällaisia verkkoyhtiöiden sovelluskohteita ovat energiatietojen kaukoluku, hälytysten välittäminen, etävideovalvonta, tariffi- ja erotinohjaukset [4]. Käytetyt tekniikat ovat GSM (2G, Global System for Mobile Communication), GPRS (General Packet Radio Services), UMTS- tekniikka (3G, Universal Mobile Telecommunications Service) sekä SMS (Short Message Service) [1].

GSM- ja GPRS- tekniikka pohjautuu toisen sukupolven matkapuhelintekniikkaan ja on toiminnaltaan jo melko vanhanaikaista. Muutos 2G:stä 3G:hen on jo nähtävissä etäluentamittareiden osalta. 2G- verkot tullaan lakkauttamaan lähivuosien aikana, joten niihin investoiminen ei ole enää kannattavaa. Kolmannen sukupolven verkoista käytetään nimitystä UMTS. UMTS pohjautuu WCDMA- tekniikkaan (Wideband Code Division Multiple Access), jossa radiorajapintaa kyetään hyödynnetään GPRS-tekniikkaa paremmin. UMTS- ja GPRS- tekniikka eroaa merkittävästi toisistaan radioverkon osalta. WCDMA- tekniikan ansiosta, vierekkäisten tukiasemien on mahdollista hyödyntää samoja taajuusalueita, joihin GSM- tekniikka ei kykene [6].

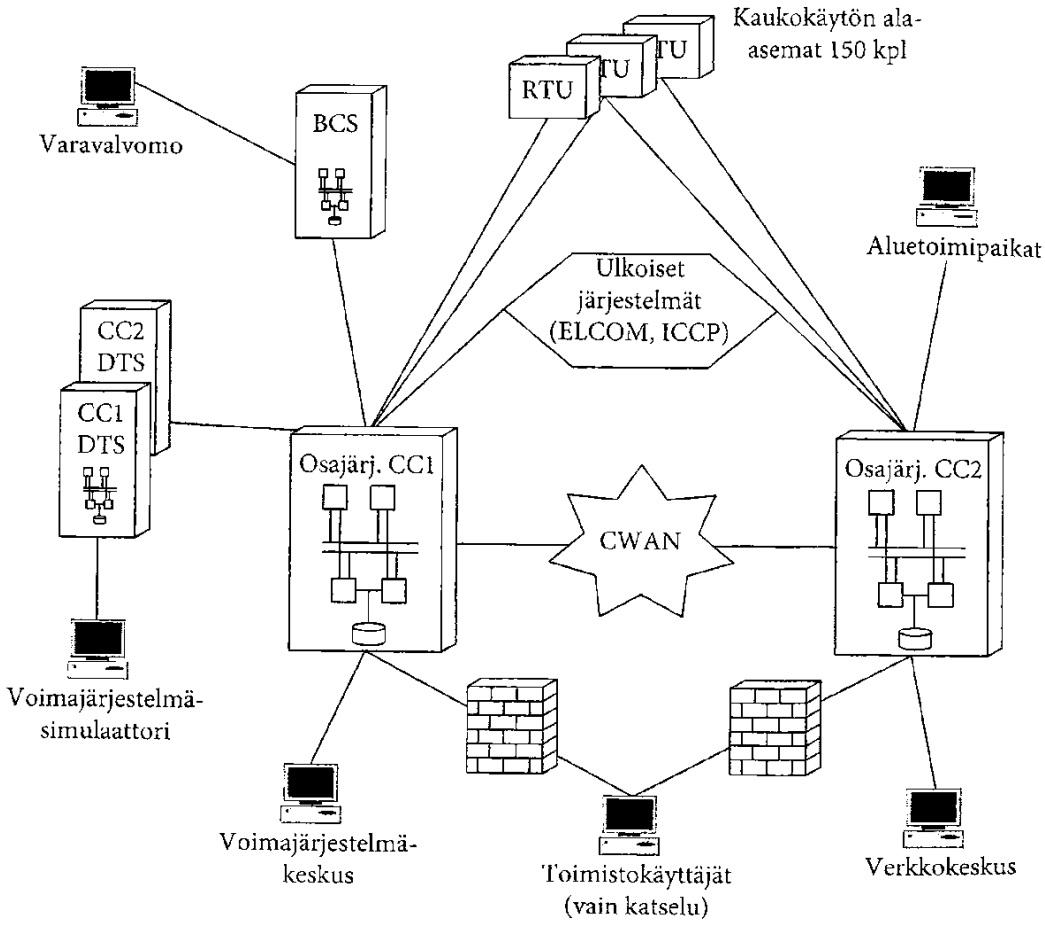
Langattomassa tiedonsiirrossa on huomioitava, että langattomuus sisältää tarpeelliset työkalut turvallisen yhteyden muodostamiseen. Ongelmallisina kohteina voidaan pitää sulautettuja laitteita, joiden suorassa langattomassa yhteydessä ei ole resursseja vahvaan salaukseen tai VPN- yhteyksien muodostamiseen [1].

3.2 Liikennöintiprotokollat

Sähkönjakeluautomaation käytössä olevien protokollien ensisijainen tarkoitus on tiedonsiirtokaistan minimoiminen. Niiden pääasiallinen käyttö kohdistuu ala- asemien ja tietojärjestelmien väliseen kommunikointiin. Tietojärjestelmien väliseen tiedonsiirtoon käytetyt tekniikat perustuvat lähtökohtaisesti yhtiöiden omiin ratkaisuihin. Poikkeuksen tekevät valvomoiden välinen tiedonsiirto, jossa pääsääntöisesti käytetään vakiintuneita spesifikaatioita [1,7].

SCADA- järjestelmä käyttää tiedonsiirtoon TCP/ IP- protokollaa (Transmission Control Protocol/ Internet Protocol), jossa verkon solmulla on oma staattinen IP- osoite. IP- osoite muodostuu neljästä numerosta, väliltä 0- 255. On olemassa myös erikoisia IP- osoitteita kuten 127.0.0.1, jolla viitataan koneeseen itseensä [5].

Hajautetussa SCADA- järjestelmässä kuvassa 4. , kahden käytönvalvontajärjestelmän välinen yhteydenpito on hoidettu ELCOM- (Electricity Utilities Communications) tai ICCP- protokollalla (ICCP, Inter Control Center Communications Protocol) [5].



Kuva 4. Hajautettu SCADA- järjestelmä [5].

ICCP- protokolla tunnetaan Euroopassa paremmin nimellä TASE.2, joka on sähköalan kansainvälisen standardisoimisjärjestön (IEC) standardoima [4].

ELCOM-90- protokolla on reaaliaikaisen aikaleimatun tiedonvaihdon protokolla. Sen käyttö on yleistä mittaustietojen ja kytkinlaiteiden tilatietojen siirrossa. Se sijoittuu OSI- järjestelmässä (Open System Interconnection) TCP/ IP- protokollan päälle. Sen pääasiallinen tehtävä on informaation siirtäminen eri valvontakeskusten välillä. OSI-järjestelmän malli on kuvassa 5 [8].

Kuva 5. OSI- mallin kerrokset [8].

Muita tunnettuja käytössä olevia protokollia on mm. IEC 60870- 5- protokollaperheeseen kuuluva DNP3 (Distributed Network Protocol). Se sallii liikennöinnin eri SCADA- valmistajien komponenttien välillä. DNP3 – protokolla toimii OSI- mallissa TCP/ IP- verkon päällä ja on yksi käytetyimmistä IED- laitteiden (Intelligent Electronic Device) väliseen tiedonsiirtoon. DNP3- protokolla soveltuu myös RTU- laitteiden, ala- asemien ja valvontakeskusten väliseen liikennöintiin [9].

Sarjaliikenneprotokolla Modbus on kehitetty PLC- laitteiden (Programmable Logic Controller) väliseen liikennöintiin. Se sijoittuu OSI- mallissa 7. Tasolle. Modbus- protokolla sisältää kaksi liikennöintitilaa, RTU (Remote Terminal Unit) ja ASCII (American Standard Code for Information Interchange) [10].

Kaukokäytön ala- asemien runsaslukuisuudesta johtuen, ne on liitetty tiedonkeruupalvelimiin. Tästä johtuen, niiden tulee kyetä toimimaan monella eri protokolla- tasolla. Yhä enenevässä määrin käytetään IEC 60870 – 101 protokollaa.

IEC 101- protokollassa on käytössä valmiit tietotyypit mm. suojauslaitteille sekä jännitesäätimille. 101- protokollan lisäksi, käytönvalvontajärjestelmä tukee TCP/ IP- pohjaista IEC 60870- 104- protokollaa [10].

3.3 Tietokannat

Käytönvalvontajärjestelmä hyödyntää toiminnassaan historiatietokantoja, joihin mittaus- ja tapahtumatiedot on kerätty. Tietokantaan tallennetaan ainoastaan uusimmat tiedot tietyltä ajanjaksolta. Tietokannalta edellytetään luotettavuutta ja joustavuutta, jotta sen käyttö olisi mahdollista myös muissa sovelluksissa.

3.4 Ohjelmistot

SCADA- järjestelmän ohjelmisto koostuu kolmesta ohjelmasta; perusohjelma, apuohjelma sekä sovellusohjelma. Sovellusohjelman yhtenä sovelluksena voi toimia esimerkiksi sähkön- tai kaasunjakelu. Kyseiset ohjelmat on nykyään lähes kaikki täysgraafisia ja siten melko helppokäyttöisiä.

Käytönvalvontajärjestelmän sovelluksilla on käytössään lisäksi varjosovellus, johon päivitetään levytiedostoissa ja keskusmuistissa olevien tietojen muutokset. Tästä päivityksestä käytetään nimitystä kuumavarmennus (Hot Stand-by) [11].

4. AUTOMAATTINEN MITTARINLUENTA JA TIEDONSIIRTO

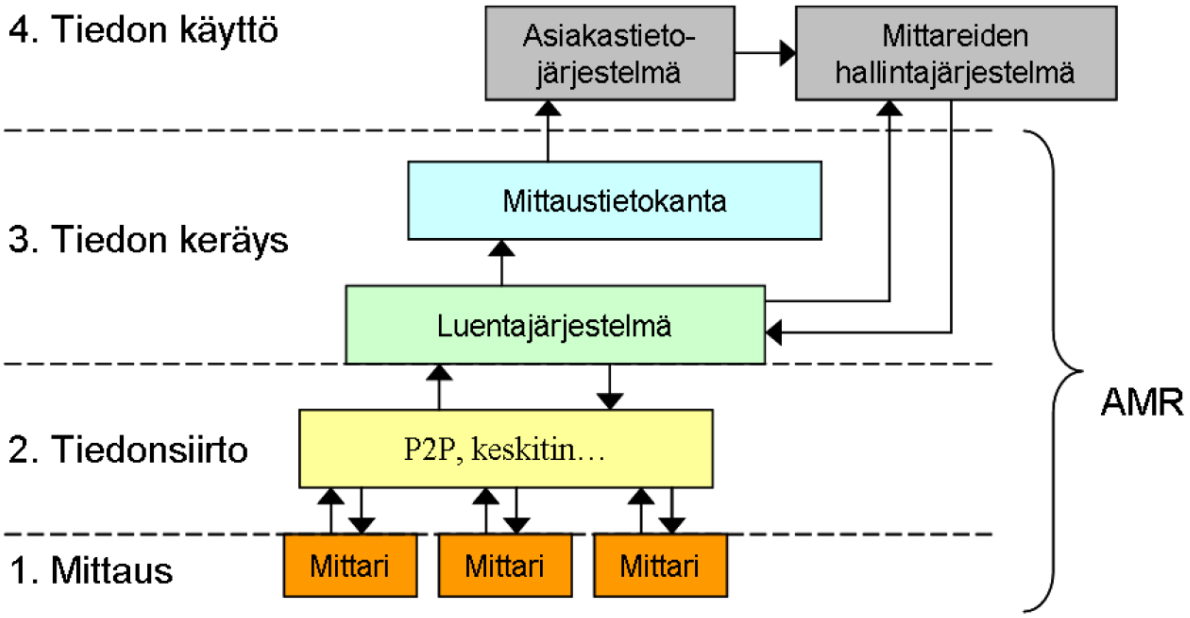
Älykäs mittarointi on osa älykästä energiaverkkoa. Asiakasliittymään sijoitettu energiamittari on älykäs mittaus- ja toimilaite, joka sisältää energianmittauksen lisäksi älyyn ja tehoelektroniikkaan perustuvia toimintoja. Tiedonsiirrossa on käytössä monenlaisia eri tekniikoita ja erilaisia arkkitehtuureja. Tässä luvussa tarkastellaan sähköverkkoon kytkettyjä etäluettavia mittareita sekä niiden tiedonsiirtoa. Lisäksi tarkastellaan kriittiseen tiedonsiirtoon pohjautuvaa DSiP- järjestelmää.

4.1 Etäluettavat sähkömittarit

Suomessa, suurimpaan osaan kotitalouksia, on jo ehditty asentaa ns. älykäs energianmittausjärjestelmä. Tätä kehitystä on ollut nopeuttamassa Suomen Valtioneuvoston antama asetus 1.3.2009/ 66, jonka mukaan vuoden 2013 loppuun mennessä, 80% kotitalouksien sähkönmittauksista on perustuttava etäluentaan. Näitä etäluettavia energiamittareita kutsutaan AMR- mittareiksi (Automatic Meter Reading).

AMR- mittareiden ensisijainen tavoite on tuottaa kustannussäästöjä energiayhtiölle sekä vähentää manuaalisen työn vaiheita, kuten henkilökohtaiset mittariluentakäynnit ja muut säätötoimet. Kustannussäästöjen lisäksi mittareilla kyetään havaitsemaan mahdolliset sähkövarkaudet. Uusimpien AMR- mittareiden ohjattavat releet mahdollistavat lisäksi erilaisia kuormanohjauksia [12].

Etäluettavat sähkömittarit ovat osa suurempaa infrastruktuurikokonaisuutta, josta käytetään nimitystä älykäs mittarointi, AMI (Advance Metering Infrastructure). Tähän kuuluu AMR- mittareiden lisäksi, tiedonsiirto sekä mittaus- ja mittaritiedon hallintaan käytetyt tietojärjestelmät. Älykäs mittarointi voidaan jakaa neljään toiminnalliseen tasoon, joita ovat alueellinen mittarinluenta, tiedonsiirto verkkoyhtiön ja mittarin luentaan käytettävien keskittimien välillä, tiedonkeräys sekä tietojärjestelmien ja sähkömarkkinaosapuolien välinen tiedon käyttö. Älykkään mittaroinnin rakennetta on esitetty kuvassa 6 [6].



Kuva 6. Kerroksittainen AMR- järjestelmä [6].

Etäluettavien mittareiden älykkyys perustuu kahdensuuntaiseen tiedonsiirtoon. Tyypillisiä toimintoja ovat:

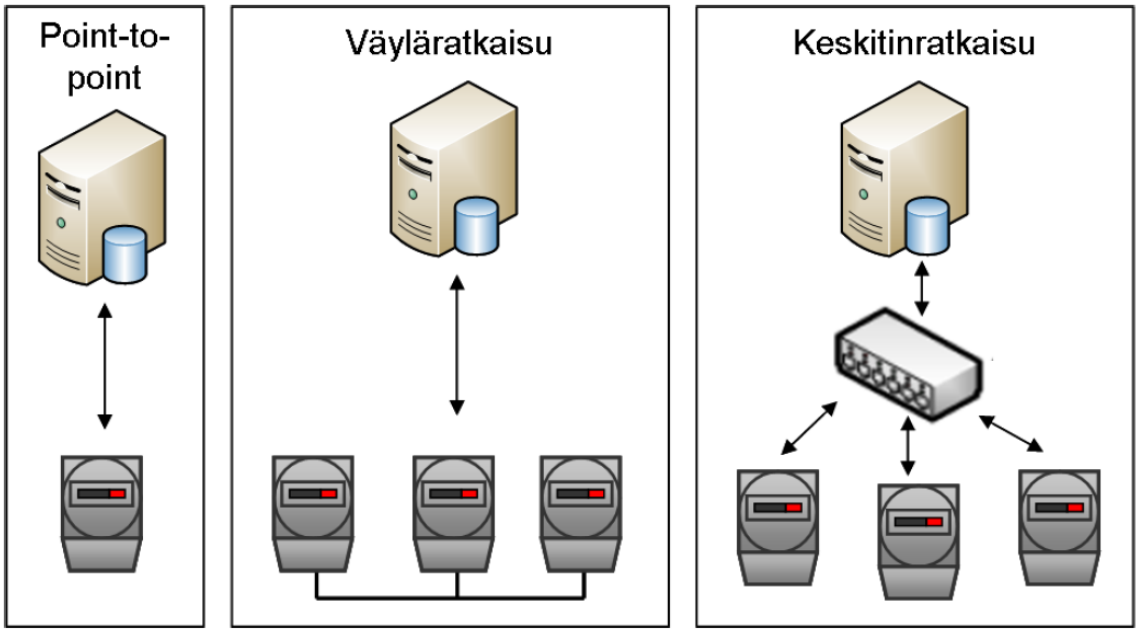
- keskeytysten rekisteröinti
- kuormanohjaus
- mittareiden päivitys
- jännitteen mittaus

4.2 Mittareiden tiedonsiirto

Automaattisessa mittariluentajärjestelmässä on käytössä kolme erilaista tiedonsiirtotapaa, jotka perustuvat mittareiden lukumäärään. Tapauksesta, jossa mittareita on harvassa, kuten haja- asutusalueilla, puhutaan suorasta tiedonsiirrosta. Tämä tunnetaan myös nimellä point-to-point- tiedonsiirto.

Väyläratkaisuarkkitehtuurissa, on kyse useamman mittarin yhteen kytkemisessä siten, että yhden mittarin väylään liittäminen, toimii yhdyskäytävänä muille mittareille.

Keskitinratkaisu- arkkitehtuuri sopii järjestelmälle, jossa mittareita esiintyy tiheästi. Siinä tiedonsiirto mittarien ja keskittimen välillä tapahtuu radio- tai sähköverkkotiedonsiirrolla. Tiedonsiirron arkkitehtuuria on havainnollistettu kuvassa 7 [6].



Kuva 7. AMR- järjestelmän tiedonsiirtoa [6].

Kappaleessa 3.1 on esitelty yksityiskohtaisemmin sähköverkon tiedonsiirtotekniikoita, jotka ovat yleisesti käytössä myös etäluettavien mittareiden tiedonsiirrossa.

4.3. DSiP- järjestelmä

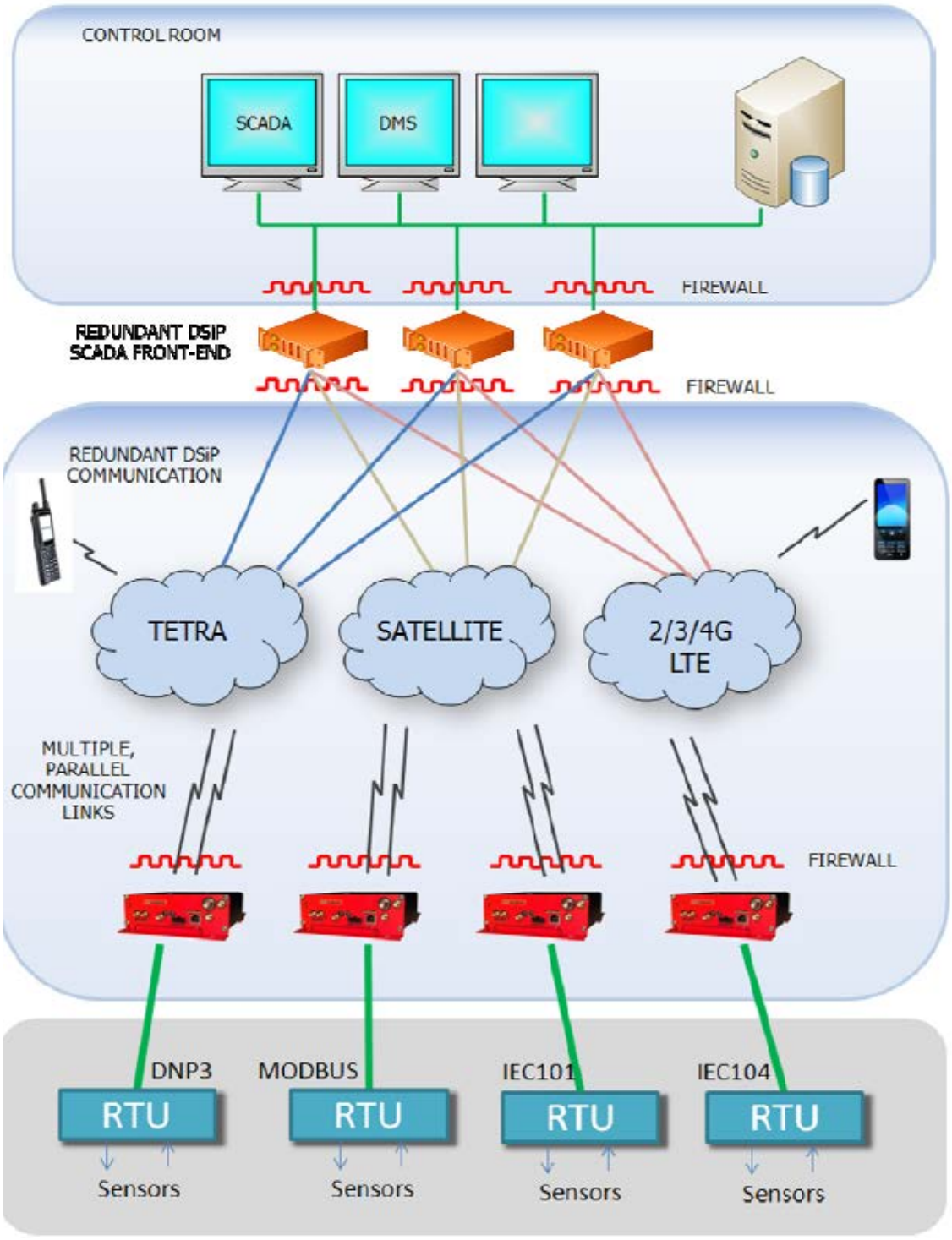
DSiP- järjestelmä (Distributed Systems Intercommunication Protocol) kykenee tarjoamaan luotettavaa tiedonsiirtoa monikanavareititinympäristössä. Järjestelmän toiminta pohjautuu IP- protokollaan, jonka avulla kyetään luomaan luotettava ja vikasietoinen tiedonsiirtojärjestelmä IP- ympäristössä. Sähköverkon kaukohallintakytkennät ovat osa kriittistä tiedonsiirtoympäristöä, johon DSiP- järjestelmällä kyetään saamaan ratkaisu.

DSiP- järjestelmää käytetään muun muassa teollisuuden ohjausjärjestelmissä, SCADA- järjestelmän sovelluksissa sekä muissa turvallisuutta vaativissa sovelluksissa [13].

Monikanavareititysympäristössä olevien kohteiden on mahdollista ylläpitää yhteyttä keskenään, edellä esitettyjä tiedonsiirtomenetelmiä hyväksikäyttäen.

DSiP- järjestelmä kykenee luomaan tiedonsiirtoyhteyden monen erilaisen yhteyskäytännön kautta, jopa siten, että moni eri tekniikka on käytössä samaan aikaan.

Tämä tapa mahdollistaa verkon tiedonsiirtokapasiteetin suuremman käytön. DSiP-järjestelmän rakennetta SCADA- järjestelmän ympäristössä on havainnollistettu kuvassa 8 [13].



Kuva 8. DSiP- järjestelmä SCADA- ympäristössä [13].

DSiP- järjestelmä perustuu verkkoympäristössä toimiviin DSiP- nodeihin; päätelaitteisiin kuten etäluettavat mittarit, kytkimet, releet, jotka kykenevät säilyttämään yhteyden reitittimeen huolimatta siitä, että yksi tai useampi

tiedonsiirtoväylä on poikki. Päätelaitteet kykenevät kytkeytymään erittäin nopeasti takaisin reitittimeen eikä turhia tiedonsiirtokatkoksia pääse syntymään [13].

DSiP- järjestelmän tuomia etuisuuksia ovat [13]:

- järjestelmän immuniteetti verkon DoS- hyökkäyksille
- tiedonsiirron läpinäkyvyys DNP3, IEC101/104, MODBUS- protokollien välillä
- eri verkkotekniikoiden samanaikainen käyttö (LAN/WAN, TETRA, 2/3/4G)
- alentunut riski viruksille
- automaattinen uudelleen reititys

4.4. Tietoturvastandardit

Standardeilla pyritään sähköverkkoteollisuudessa käytettävyyden, turvallisuuden ja luotettavuuden parantamiseen. Kansainvälisiä sähköalan standardoimisjärjestöjä ovat IEC (*International Electrotechnical Commission*), IEEE (*Institute of Electrical and Electronics Engineers*), NIST (*National Institute of Standards and Technology*), NERC (*North American Electric Reliability Corporation*) sekä CPNI (*Centre for Protection of National Infrastructure*). Standardien tehtävä on parantaa sähkö- ja tietoturvallisuutta mutta niiden yleisenä ongelman on pidetty sitä, että niistä on vaikeaa tunnistaa kuhunkin tarpeeseen parhaiten soveltuvat ratkaisut [14].

Verkostoautomaatiolle tärkeitä standardeja on esitetty taulukossa 1.

Taulukko 1. Verkostoautomaatiostandardeja [14].

Standardi/ normi/ohje	Sovellusalue	Status	Käyttökohde
ISO/IEC 270xx, xx= 00…37	Kansainvälinen standardi, hyvin kattava	-01, -02 ja -05 laajasti käytössä	Yleinen IT-ohjeistus ja vaatimukset tietoturvan hallintaan yms.
IEC 62351	Kansainvälinen tekninen spesifikaatio	Julkistettu, soveltaminen käynnistynyt	Verkostoautomaatio-järjestelmien data- ja protokollasuojaus
IEEE 1711	IEEE standardi, globaalisti relevantti	Julkistettu, soveltaminen käynnistynyt	Erityisesti ala-asemien perinteisen sarjaliikenteen salaaminen
IEEE 1686	IEEE standardi, globaalisti relevantti	Julkistettu, soveltaminen käynnistynyt	Kenttälaitteiden vaatimusmäärittely, perustuu NERC CIP -vaatimuksiin
ANSI/ISA-99 IEC 62443	USA-lähtöinen, globaalisti relevantti	Osa julkistettu. Työ jatkuu	Teollisuusautomaatio-järjestelmien ja verkkojen tietoturvan toimintamallit yms.
NIST SP800-82	USA-lähtöinen, globaalisti relevantti	Julkistettu ja käytössä laajasti	Guide for Industrial Control System (ICS) Security, tietoverkkoinfrastruktuurin kybersuojaus
NERC CIP	USA ja Kanada, globaalisti relevantti	Julkistettu, pakollinen amerikkalaisille voimayhtiöille	Tietoverkkoinfrastruktuurin kybersuojauksen suunnittelusääntöjä ja toimintaohjeita
CPNI suositukset	Iso-Britania, globaalisti relevantti	Julkistettu, käytössä	Kybersuojauksen viitekehys ja hyvät käytännöt
COREQ-VE, COREQ-ACT	Suomi	Käytössä	Teollisuusautomaatio-järjestelmän tietoturvavaatimuksia

5. KYBER

Mitä ymmärrämme kyber- alkuisella sanalla? Sana esiintyvät nykyään monessa eri muodossa, kuten kyberavaruus, kyberterrorismi, kyberuhka, kyberhyökkäys, kyberturvallisuus mutta mitä sillä oikeastaan tarkoitetaan? Lähdetään liikkeelle kybernetiikasta, joka märitellään itseohjautuvia järjestelmiä tutkivaksi tieteeksi, ja jota hyödynnetään muun muassa teknisten järjestelmien mallinnuksessa. Kyber- sanan katsotaan olevan lähtöisin kreikankielen sanasta "kybereo", joka tarkoittaa opastusta, ohjaamista. Sana itsessään esiintyy usein perusosan ja määriteosan yhdistelmänä, joka antaa sille todellisen sisältömerkityksen. Kyber voidaan tulkita eräänlaisena sähköisen muodon informaatiokäsittelynä. Se liittyy osana tietotekniikkaan, sähköiseen viestintään, kriittisen tuotannon kontrollointiin sekä tieto- ja tietokonejärjestelmiin. Perinteisen tietoturvan ja kyberturvan eroavaisuus ilmenee siinä, että perinteisessä tietoturvassa keskitytään tiedon luottamuksellisuuteen, eheyteen ja saatavuuteen kun taas kyberturvallisuudessa käsite on huomattavasti kattavampi. Kyberturvallisuuden piiriin katsotaan kuuluvaksi koko infrastruktuurimme, lähtien liikkeelle fyysisistä laitoksista ja rakenteista sekä sähköisistä toiminnoista ja palveluista [15].

Kyberverkko on maailmanlaajuinen tietoverkko, josta käytetään myös nimitystä kyberavaruus. Se muodostuu kaikista maailman eri toimijoiden verkoista ja laitteista, jotka ovat verkon välityksellä kytkeytyneet toisiinsa. Tällaisia verkkoja ovat kansalliset viranomaisverkot, yritysverkot sekä teollisuuden automaatiojärjestelmien verkot [15].

5.1. Suomen kyberturvallisuusstrategia

Kasvava huoli yhteiskuntaturvallisuudesta on saanut valtiovallan turvaamaan yhteiskuntamme etuja kyberturvallisuusstrategialla. Valtioneuvoston 24.1.2013 julkaisemassa kyberturvallisuusstrategiassa, kyberturvallisuus määritellään tavoitetilaksi, jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan.

Kyberturvallisuusstrategian syntymiseen on vaikuttanut viimeaikainen tietoyhteiskunnan kehitys, jossa kybertoimintaympäristöön kohdistuvat uhat ovat muuttuneet yritysten ja yhteiskunnan kannalta aiempaa vaarallisemmiksi.

Kybertoimintaympäristön uhkia muodostavat perinteisten haktivistien lisäksi myös valtiolliset toimijat, joiden tarkoitusperät voivat olla joko poliittisia tai sotilaallisia.

Kybertoimintaympäristöön kohdistuviin haasteisiin pyritään vastaamaan strategisilla linjauksilla, toimintamalleilla ja visioilla ja tällä tavalla estämään kybertoimintaympäristön tahalliset tai tahattomat haittavaikutukset ja loukkaukset [16].

5.1.1 Kyberturvallisuuden visio

Kyberturvallisuuden visiossa, Suomen katsotaan olevan kolmen vuoden kuluttua johtavia maita kyberturvallisuuden kehittämisessä sekä maailmanlaajuinen edelläkävijä tietoverkkoihin kohdistuviin uhkiin varautumisessa ja niiden häiriöiden hallinnassa. Suomella on lisäksi kyky suojata elintärkeät toimintonsa kaikissa tilanteissa [16].

5.1.2 Kyberturvallisuuden toimintamalli

Kyberturvallisuuden toimintamalli nojautuu kahdeksaan periaatteeseen, joiden avulla kyetään luomaan kokonaisturvallisuuden mukainen varautumis- ja ennakointikyky. Periaatteita ovat [16]:

1. Kyberturvallisuuden asiat kuuluvat pääsääntöisesti valtioneuvoston toimivaltaan siten, että tehtävät on säädetty eri ministeriöiden toimialalle. Kukin ministeriö vastaa toimialallaan valtioneuvostolle kuuluvien, kyberturvallisuuteen liittyvien asioiden valmistelusta ja hallinnon asianmukaisesta järjestämisestä.

2. Kyberturvallisuus on kiinteä osa yhteiskunnan kokonaisturvallisuutta ja sen toimintamalli noudattaa Yhteiskunnan turvallisuusstrategiassa (YTS) määritettyjä periaatteita ja toimintatapoja.

3. Kyberturvallisuus perustuu koko yhteiskunnan tietoturvallisuuden järjestelyihin. Kyberturvallisuuden edellytys on jokaisen kybertoimintaympäristössä toimivan toteuttamat tarkoituksenmukaiset ja riittävät tietojärjestelmien ja tietoverkkojen turvallisuusratkaisut. Näiden toteuttamista edesautetaan ja tuetaan erilaisten yhteistoimintaan perustuvien rakenteiden ja harjoitusten avulla.

4. Kyberturvallisuuden toimintamalli perustuu tehokkaaseen ja laaja-alaiseen tiedon hankinta-, analysointi- ja keruujärjestelmään, yhteiseen ja jaettuun tilannetietoisuuteen sekä kansalliseen ja kansainväliseen yhteistoimintaan varautumisessa. Tämä edellyttää kansallisen Kyberturvallisuuskeskuksen perustamista sekä koko yhteiskunnan ympärivuorokautisen tietoturvatoiminnan kehittämistä.

5. Kyberturvallisuuden järjestelyissä noudatetaan viranomaisten, yritysten ja järjestöjen välillä vastuunjakoa, joka perustuu säädöksiin ja sovittuun yhteistyöhön. Tarve sopeutua nopeisiin muutoksiin, kyky hyödyntää uusia mahdollisuuksia ja reagoida yllättäviin tilanteisiin vaatii toimijoilta strategisen ketteryyden periaatteiden ymmärtämistä ja noudattamista kyberturvallisuuteen tähtäävien toimien kehittämisessä ja johtamisessa.

6. Kyberturvallisuutta rakennetaan toiminnallisten ja teknisten vaatimusten perusteella. Kansallisten toimenpiteiden lisäksi panostetaan kansainväliseen yhteistoimintaan ja osallistutaan kansainväliseen tutkimus- ja kehittämistoimintaan sekä harjoitustoimintaan. Kyberturvallisuuteen tähtäävän tutkimuksen, kehittämisen ja koulutuksen toteuttaminen eri tasoilla vahvistaa kansallista osaamista ja Suomea tietoyhteiskuntana.

7. Kyberturvallisuuden kehittämisessä panostetaan voimakkaasti kybertoimintaympäristön tutkimukseen, koulutukseen, työllistymiseen ja tuotekehitykseen, jotta Suomi voisi kehittyä yhdeksi kyberturvallisuuden johtavista maista.

8. Kyberturvallisuuskehityksen varmistamiseksi huolehditaan siitä, että Suomessa on voimassa sellainen lainsäädäntö ja kannustimet, jotka tukevat tämän alueen yritystoimintaa ja sen kehittymistä. Alan osaaminen kehittyy keskeiseltä osaltaan yritystoiminnan kautta.

5.1.3 Kyberturvallisuuden strategiset linjaukset

Kyberturvallisuuden strategisilla linjauksilla pyritään luomaan toteutumisen edellytykset eri visioille. Strategiset linjaukset on kirjattu periaatepäätökseen seuraavasti [16]:

1. Luodaan kansallisen kyberturvallisuuden ja kyberuhkien torjunnan edistämiseksi viranomaisten ja muiden toimijoiden välinen tehokas yhteistoimintamalli.

Kyberturvallisuusstrategian strategisia linjauksia edistetään lisäämällä toimijoiden välistä aktiivista yhteistoimintaa, jonka tavoitteena on jaettu tilannetietoisuus ja tehokas uhkien torjunta. Eri toimialojen valmiutta toimia elintärkeiden toimintojen häiriötilanteissa harjoitellaan säännöllisesti. Jokainen toimija kehittää kansallista ja kansainvälistä osallistumista harjoitustoimintaan. Toimijat parantavat kansainvälisissä harjoituksissa parhaiden käytänteiden ja saatujen oppien hyödyntämistä tehostamalla tiedonvaihtoa ja koordinaatiota. Harjoitustoiminnan tavoitteena on parantaa osallistujien mahdollisuuksia havaita oman toimintansa ja järjestelmiensä haavoittuvuuksia, kehittää suorituskykyjään ja kouluttaa henkilöstöään. Kyberuhkien torjumiseksi tiedonvaihtoa viranomaisten ja elinkeinoelämän kesken edistetään kehittämällä sääntelyä ja yhteistyötä.

2. Parannetaan yhteiskunnan elintärkeiden toimintojen turvaamiseen osallistuvien keskeisten toimijoiden kokonaisvaltaista kyberturvallisuuden tilannetietoisuutta ja tilanneymmärrystä.

Tavoitteena on parantaa eri toimijoiden tilannetietoisuutta tarjoamalla niille ajantasaista, koottua ja analysoitua tietoa haavoittuvuuksista, häiriöistä ja niiden vaikutuksista. Tilannekuvaan sisältyy kybertoimintaympäristöstä aiheutuvien uhkien arviot ja ennusteet. Kyberuhkien ennakointi edellyttää poliittisen, sotilaallisen, sosiaalisen, kulttuurisen, teknisen ja teknologisen sekä taloudellisen tilanteen arviointia. Yhdistetyn kyberturvallisuuden tilannekuvan tuottamiseksi ja ylläpitämiseksi perustetaan Kyberturvallisuuskeskus, joka toimii osana Viestintävirastoa. Kyberturvallisuuskeskus kerää tietoa kybertapahtumista ja välittää sitä eri toimijoille. Toimijat arvioivat häiriön vaikutuksia vastuullaan olevaan toimintaan. Nämä analyysit välitetään takaisin keskukselle ja sisällytetään muodostettavaan kyberturvallisuuden yhdistettyyn tilannekuvaan. Tämä koonnos jaetaan päätöksenteon pohjaksi eri toimijoille. Valtioneuvoston tilannekeskuksella tulee olla käytettävissään luotettava, kattava ja ajantasainen kokonaistilannearvio kyberturvallisuudesta. Arvio koostuu Kyberturvallisuuskeskuksen yhdistetystä tilannekuvasta sekä hallinnonalojen arvioista kybertapahtumien vaikutuksista yhteiskunnan elintärkeille toiminnoille. Valtionjohdolla on käytettävissään kokonaistilannearvio sekä arvio muun toimintaympäristön kehityksestä.

3. Ylläpidetään ja kehitetään yhteiskunnan elintärkeiden toimintojen turvaamisen kannalta tärkeiden yritysten ja organisaatioiden kykyä havaita ja torjua elintärkeää toimintoa vaarantavat kyberuhkat ja -häiriötilanteet sekä toipua niistä osana elinkeinoelämän jatkuvuuden hallintaa.

Yhteiskunnan elintärkeiden toimintojen kannalta keskeiset yritykset ja organisaatiot ottavat turvallisuus- ja valmiussuunnittelussaan sekä niihin liittyvissä palvelurakenteissa kattavasti huomioon yhteiskunnan elintärkeisiin toimintoihin liittyvät kyberuhkatekijät ja pitävät yllä tarvittavaa suojautumiskykyä. Tavoitteena on, että riskiarvioissa esiin tulleet elintärkeiden toimintojen mahdolliset häiriöt tunnistetaan ja havaitaan, ja niihin reagoidaan tavalla, joka minimoi häiriöiden haitalliset vaikutukset. Keskeiset toimijat kehittävät sietokykyään, mukaan lukien varamenetelmien suunnittelu ja harjoittelu niin, että ne voivat toimia kyberhyökkäysten alaisena. Huoltovarmuusorganisaatio tukee toimintaa selvityksin, ohjeistuksin ja koulutuksella.

4. Huolehditaan, että poliisilla on tehokkaat edellytykset ennalta ehkäistä, paljastaa ja selvittää kybertoimintaympäristöön kohdistuvia ja sitä hyödyntäviä rikoksia.

Kybertoimintaympäristöön kohdistuvien ja sitä hyödyntävien rikosten esitutkintaviranomaisena toimii poliisi. Poliisi kokoaa analysoidun ja korkealaatuisen tilannekuvan kyberrikollisuudesta ja jakaa sen osaksi strategisessa linjauksessa 2 kuvattua yhdistettyä tilannekuvaa.
Poliisi toimii tiiviissä yhteistyössä Kyberturvallisuuskeskuksen kanssa.
Huolehditaan, että poliisilla on riittävät toimivaltuudet, resurssit sekä osaava ja motivoitunut henkilöstö, joka hoitaa kybertoimintaympäristöön kohdistuvien ja sitä hyödyntävien rikosten ennaltaehkäisemisen, taktisen esitutkinnan sekä digitaalisen todistusaineiston käsittelyn ja analysoinnin.
Jatketaan ja syvennetään kansainvälistä operatiivista yhteistyötä ja tiedonvaihtoa EU:n ja muiden maiden lainvalvontaviranomaisten ja vastaavien toimijoiden kuten Europolin kanssa.

5. Puolustusvoimat luo kokonaisvaltaisen kyberpuolustuskyvyn lakisääteisissä tehtävissään.

Sotilaallinen kyberpuolustuskyky muodostuu tiedustelun, vaikuttamisen ja suojautumisen suorituskyvyistä. Puolustusvoimat suojaa omat järjestelmänsä siten, että se kykenee suoriutumaan lakisääteisistä tehtävistään huolimatta kybertoimintaympäristön uhkista. Suorituskyvyn varmistamiseksi kehitetään tiedustelu- ja vaikuttamiskykyä kybertoimintaympäristössä osana muun sotilaallisen voimankäytön kehittämistä. Edellä mainittujen tehtävien täyttämiseksi laaditaan puolustusministeriön johdolla puolustusvoimille tarvittava toimivaltuussäännöstö. Tunnistetut puutteet toimivaltuussäädöksissä korjataan lainsäädäntötoimenpitein. Kyberpuolustusta harjoitellaan ja kehitetään yhdessä keskeisten viranomaisten, järjestöjen ja elinkeinoelämän toimijoiden kanssa kansallisesti ja kansainvälisesti. Puolustusvoimat antaa virka-apua lainsäädännön salliessa.

6. Vahvistetaan kansallista kyberturvallisuutta osallistumalla aktiivisesti ja tehokkaasti kyberturvallisuuden kannalta keskeisten kansainvälisten organisaatioiden ja yhteistyöfoorumeiden toimintaan.

Kansainvälisen yhteistoiminnan tavoitteena on vaihtaa tietoja ja kokemuksia sekä oppia parhaista käytännöistä, jotta kansallisen kyberturvallisuuden tasoa voidaan kohottaa. Varautumisen ja muun kyberturvallisuuden toteuttaminen jää vaillinaiseksi ilman tehokasta ja järjestelmällisesti koordinoitua kansainvälistä yhteistyötä.

Jokainen viranomainen omalla toimialallaan harjoittaa yhteistyötä erityisesti niiden valtioiden ja organisaatioiden kanssa, jotka ovat maailmanlaajuisesti edelläkävijöitä kyberturvallisuuteen liittyvissä asiakokonaisuuksissa. Aktiivista yhteistyötä tehdään tutkimus- ja kehittämistyön, erilaisten sopimusten valmistelutyön, organisaatioiden työryhmätyöskentelyn, sekä kansainväliseen harjoitustoimintaan osallistumisen kautta. Euroopan unioni sekä monet kansainväliset järjestöt, kuten YK, ETYJ, Nato ja OECD, ovat Suomelle tärkeitä foorumeita kyberturvallisuutta kehitettäessä. EU toimii yhä aktiivisemmin kyberturvallisuuden alalla ja sillä on myös yhteistyötä kolmansien maiden kanssa. Suomi osallistuu aktiivisesti tähän kehittämistyöhön.

7. Parannetaan kaikkien yhteiskunnan toimijoiden kyberosaamista ja -ymmärrystä.

Yhteiskunnan toimijoiden jatkuvan osaamisen ja tietämyksen kehittämisen tukena panostetaan yhteisten kyberturvallisuuden ja tietoturvallisuuden ohjeistojen kehittämiseen, hyödyntämiseen ja kouluttamiseen. Yhteiskunnan kokonaisvaltaisen valmiuden kehittämiseksi harjoitustoimintaan otetaan mukaan myös yhteiskunnan elintärkeiden toimintojen kannalta tärkeät yritykset ja kansalaisjärjestöt.

Perustetaan olemassa olevan ICT-SHOKin (TIVIT) yhteyteen kyberturvallisuuden strateginen huippuosaamisen keskittymä, joka tarjoaa tutkimusyksiköille ja tutkimustuloksia hyödyntäville yrityksille tehokkaan tavan tehdä tiivistä ja pitkäjänteistä yhteistyötä keskenään. Keskittymä luo edellytyksiä vahvan kansallisen kyberosaamisklusterin rakentumiselle. Lisätään panostuksia tutkimukseen, tuotekehitykseen ja koulutukseen sekä toimenpiteitä kyberturvallisuuden osaamisen kehittämiseksi koko yhteiskunnan osalta.

8. Kansallisella lainsäädännöllä varmistetaan tehokkaan kyberturvallisuuden toteuttamisen edellytykset.

Kartoitetaan kybertoimintaympäristöön ja -turvallisuuteen vaikuttava ja liittyvä lainsäädäntö sekä sen kehittämistarpeet hallinnonalojen ja elinkeinoelämän yhteistyönä. Lainsäädäntökartoituksen tuloksena ovat lainsäädännön kehittämisehdotukset, joilla edistetään kyberturvallisuusstrategian mukaisten tavoitteiden toteutumista.

Kartoituksen yhtenä tarkoituksena on se, että lainsäädäntö antaisi mahdollisuuden sekä riittävät keinot ja toimivaltuudet eri alojen toimivaltaisille viranomaisille sekä muille toimijoille toteuttaa yhteiskunnan elintärkeiden toimintojen ja erityisesti valtion turvallisuuden suojaamista kyberuhkia vastaan. Tarkasteltavaksi otetaan myös mahdolliset lainsäädännölliset ja kansainvälisistä sopimuksista johtuvien velvoitteiden aiheuttamat esteet ja rajoitteet sekä tiedon käsittelyä koskevat velvoitteet, jotka haittaavat kyberuhkien tehokkaaksi torjumiseksi tarvittavan tiedon saamista, luovuttamista ja vaihtamista eri viranomaisten ja muiden toimijoiden välillä. Tietojen keräämistä ja muuta käsittelyä koskevassa tarkastelussa arvioitaisiin lisäksi sitä onko syytä vastuuviranomaisille luoda nykyistä paremmat mahdollisuudet ennalta kerätä, koota ja saada tietoa kyberuhista ja niiden aiheuttajista kiinnittämällä samalla huomiota perusoikeuksina olemassa oleviin yksityisyyden suojaan ja luottamuksellisen viestin suojaan. Yhteiskunnan kriittisestä infrastruktuurista on valtaosa yksityisessä omistuksessa ja liiketoiminnallisesti operoitua. Yritykset toteuttavat suurelta osin kyberkyvykkyyden, osaamisen sekä palveluiden luomisen ja suojaamisen. Kybertoimintaympäristöä säätelevän kansallisen lainsäädännön tulee olla sellaista, että liiketoiminnan kehittämiselle on olemassa suotuisat edellytykset. Tämä mahdollistaa osaltaan kansainvälisesti tunnustetun, kilpailukykyisen ja vientimahdollisuudet omaavan kyberosaamisklusterin syntymisen. Samalla Suomesta kehittyy houkutteleva kyberturvallinen toimintaympäristö, johon kannattaa tehdä investointeja ja yritysten toimintojen sijoituspäätöksiä.

9. Määritellään viranomaisille ja elinkeinoelämän toimijoille kyberturvallisuutta koskevat tehtävät ja palvelumallit sekä yhteiset perusteet kyberturvallisuuden vaatimusten hallinnalle.

Kyberturvallisuuden kehittäminen vaatii selkeää vastuiden määrittelyä ja tehtävien jakoa strategisten linjausten mukaisesti. Käytännössä tämä edellyttää, että kukin hallinnonala tekee riskiarvioinnin ja kypsyysanalyysin, joiden avulla tunnistetaan kyberturvallisuuden kannalta merkittävät haavoittuvuudet ja riskit sekä niiden hallinnan taso. Saatujen tulosten perusteella laaditaan kunkin hallinnonalan toimeenpano- ohjelmat sekä tuetaan elinkeinoelämän toimeenpano-ohjelmien tekemistä yhteistoiminnassa huoltovarmuusorganisaation kanssa.

10. Strategian toimeenpanoa valvotaan ja toteumaa seurataan.

Ministeriöt ja virastot vastaavat toimialalleen kuuluvasta strategian toimeenpanosta, kyberturvallisuuteen liittyvien tehtävien ja huoltovarmuusjärjestelyiden toteuttamisesta sekä niiden kehittämisestä. Perustettava Turvallisuuskomitea seuraa ja yhteen sovittaa strategian toimeenpanoa. Kyberturvallisuuden yhteen sovittamisen päämääriä ovat päällekkäisen toiminnan välttäminen, mahdollisten puutteiden tunnistaminen ja varmistuminen vastuutahoista. Varsinaiset päätökset tekee toimivaltainen viranomainen sen mukaisesti, mitä asiasta on säädetty.

Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmä (VAHTI) käsittelee ja yhteen sovittaa valtionhallinnon keskeiset tieto- ja kyberturvallisuuden linjaukset. Ministeriöt, virastot ja laitokset sisällyttävät kyberturvallisuusstrategian toimeenpanon edellyttämät voimavarat omiin toiminta- ja taloussuunnitelmiinsa.

5.2. Sähköverkot ja kyberturvallisuus

Internet- ja IP- teknologian kehitys teollisuusympäristössä on osaltaan ollut vaikuttamassa myös sähköverkkoyhtiöiden verkostoautomaatio- ja verkonhallintajärjestelmien rakenteeseen. Internetin, IP- protokollan ja Ethernet-pohjaisten lähiverkkojen kasvanut rooli teollisuusautomaatiolaitteiden rakennusosina sekä lisääntynyt automaatiojärjestelmien välinen tiedonsiirto on kasvattanut sähköverkkoympäristön tietoturvariskejä. Tietoturvauhat ovat lisääntyneet huolestuttavaa vauhtia, joihin myös sähköverkkoyhtiöiden on reagoitava [17].

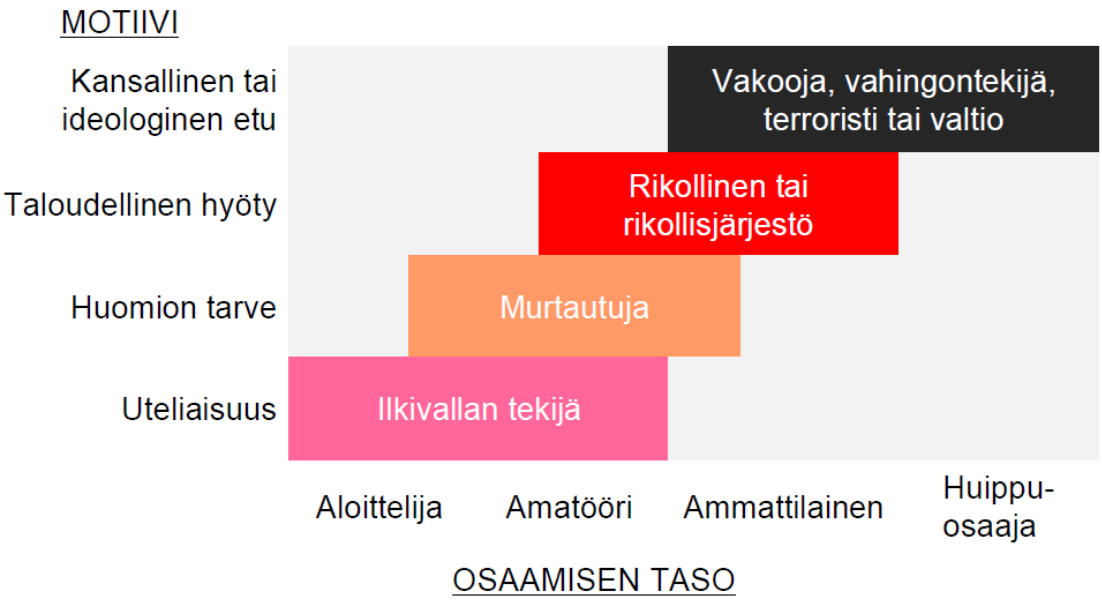
Sähköverkot ovat yhteiskuntamme infrastruktuurin keskeisimpiä tukipylväitä, minkä johdosta sähköverkkoyhtiöiltä edellytetään kattavaa varautumista tietoturvaan ja mahdollisiin kyberuhkiin. Alan toimijat ja viranomaiset ovat käynnistäneet useita hankkeita yhteiskuntaturvallisuuden takaamiseksi, josta osoituksena muun muussa edellä esitetty kyberturvallisuusstrategia [17].

Sähkönsiirrossa ja – jakelussa tietoturva on osana käytännön toimintaa ja se on yleisesti huomioitu tietoturvan vaatimuksina. Tietoturvan taso ei kaikilta osin ole kuitenkaan riittävä, sillä verkostoautomaatiojärjestelmien nopea kehittyminen lisää järjestelmien haavoittuvuuksia. Lisääntyneet kyberhyökkäykset ja toimintatapojen monipuolistuminen, on osaltaan lisännyt paineita tietoturvallisuuden parantamiselle [17].

Kyberturvallisuus voidaan ymmärtää osana tietoturvallisuutta, jota on yksityiskohtaisemmin käsitelty kappaleessa 6.3.1.

5.3 Kyberturvallisuusuhkat

Suurin uhka teollisuusautomaatioverkolle on järjestelmien parissa työskentelevät ihmiset. Työntekijöiden osaamattomuudella tai huolimattomuudella voidaan tuhota tärkeitä tietoja tai saastuttaa kokonainen järjestelmä. Toinen uhka muodostuu tietojärjestelmässä kiinni olevista laitteista ja niiden ohjelmistoista, jotka saattavat sisältää tiedostamattomia ohjelmointivirheitä. Kolmas uhka muodostuu vihamielisistä tahoista, joita on esitetty kuvassa 9.



Kuva 9. Verkon vihamieliset tahot [16].

Uhkien vakavuus on sidonnainen vihamielisen tahon osaamisen tasosta ja motiivista. Ilkivallan tekijät ovat yleensä katkeroituneita henkilöitä, jotka voivat olla esimerkiksi yhtiön entisiä työntekijöitä. Sähköyhtiön kannalta tällainen uhka katsotaan vähäiseksi.

Murtautuja tai teollisuusvakoilija pyrkii varastamaan taloudellisesti hyödynnettävissä olevia tietoja, tarjoamalla niitä kilpaileville yhtiöille. Sähköverkkoyhtiöille tämänkaltainen uhka on pieni.

Rikollisten tavoite on puhtaasti taloudellisen hyödyn saaminen. Heillä on käytössä muun muassa räätälöityjä ohjelmistoja, joiden avulla he yrittävät saada käyttäjiä tulemaan omille sivuilleen.

Terroristit ja valtiolliset toimijat ovat sähköverkkoyhtiöille vakavin uhka. Tämänkaltaisten tekijöiden ensisijainen tarkoitus on aiheuttaa huomattavan suuria aineellisia vahinkoja ja järjestelmätuhoja [1].

5.4 Sähköverkon haavoittuvuus

Sähköverkon haavoittuvuus voidaan jakaa kolmeen eri haavoittuvuusluokkaan, joita ovat:

1. Hallinnon haavoittuvuus.
2. Verkostoautomaatiojärjestelmän haavoittuvuus.
3. Tietoliikenneverkon haavoittuvuus.

Hallinnon haavoittuvuus on lähtöisin johtamistaidon puutteista, huonosta ohjeistuksesta sekä henkilöstön riittämättömästä koulutuksesta [17]. Taulukossa 2. on kuvattu ja lueteltu hallintoon liittyviä haavoittuvuuksia [17, 18].

Taulukko 2. Haavoittuvuudet hallinnossa [17].

Haavoittuvuus	Kuvaus
Tietoturvapolitiikan ja johtamisen puutteet	Verkostoautomaatiojärjestelmien erityispiirteitä ei ole huomioitu tietoturvapolitiikkaa ja –ohjeistusta laadittaessa. Verkostoautomaatiojärjestelmien tietoturvan johtamista ei ole vastuutettu. Tietoturvan systemaattista seurantaa ja säännöllistä raportointia ei ole järjestetty tai vastuutettu.
Riskikartoituksen puutteet	Toiminnan jatkuvuutta uhkaavia riskejä ei ole tunnistettu riittävästi tai ennalta ehkäiseviin toimenpiteisiin riskien vaikutusten vähentämiseksi tai eliminoimiseksi ei ole ryhdytty
Henkilöstön tietoturvaosaaminen ja tietous puutteellista	Henkilöstön koulutus ja informointi on puutteellista. Ilman ajantasaista tietoturvapolitiikkaa ja –ohjeistusta, joihin henkilöstö on perehdytetty, ei todennäköisesti rakenneta ja ylläpidetä tietoturvallista verkostoautomaatioympäristöä
Haavoittuva tietojärjestelmäarkkitehtuuri	Verkostoautomaatiojärjestelmä on rakenteellisesti puutteellinen eikä sitä ole varustettu tietoturvauhkia estävällä, tunnistavilla ja eliminoivilla laitteilla ja ohjelmistoilla. Tietoliikenneverkkoa ei ole segmentoitu ja verkostoautomaatiojärjestelmien käyttöoikeuksien hallinta on leväperäistä tai muuten riittämätöntä. Ulkoisia tietoliikenneyhteyksiä ei ole suojattu riittävästi
Järjestelmien ja laitteiden rakentamisen ja häiriöpalauttamisen ohjeistus puutteellista	Järjestelmien suunnittelussa ja rakentamisessa käytettävää ohjeistusta tietoturvan huomioimisesta ei ole tai se on puutteellista. Jatkuvuussuunnittelun tuloksena syntyviä toipumissuunnitelmia ei ole tai ne ovat puutteellisia. Järjestelmien toipumissuunnitelman laadintaa ei ole vastuutettu.
Verkostoautomaatiojärjestelmän ja sitä tukevan tietoliikenneverkon konfiguraation hallinta puuttuu tai on riittämätön	Toimiva tietoturva edellyttää jatkuvaa ja ajantasaista järjestelmien ominaisuuksien ja parametroinnin hallintaa erityisesti tehtäessä järjestelmiin muutoksia. Parametroinnit ovat puutteellisia tai virheellisiä ja käytetään järjestelmien oletusasetuksia (tehdasasetuksia)
Puuttuvat auditoinnit tai katsastukset	Ulkopuolisten riippumattomien asiantuntijoiden on auditoitava säännöllisesti verkostoautomaatio- ja tietoliikennejärjestelmien rakenne, dokumentaatio, tietoturvapolitiikka/ohjeistus sekä käytön ja ylläpidon toimintatavat ja prosessit. Auditoijien on raportoitava vakavat löydökset ja tehtävä ehdotus niiden korjaamiseksi
Puutteellinen käyttöoikeuksien hallinta	Puutteet käyttöoikeuksien hallinnoinnissa ja autentikoinnin päivityksissä (esimerkiksi salasanojen vaihtaminen) lisäävät tunkeutumisriskiä tai antavat käyttäville liian laajoja oikeuksia tehdä järjestelmään haitallisia muutoksia

Verkostoautomaatiojärjestelmän haavoittuvuus voidaan jaotella kolmeen osaan; alustan rakenteen haavoittuvuuteen, fyysisiin uhkiin sekä sovellusohjelmistojen uhkiin. Alustan rakenteen uhkiin liittyy muun muassa salasanojen paljastuminen. Fyysisiin uhkiin turvattomat ulkoiset yhteydet ja sovellusuhkiin turvattomien tietoliikenneprotokollien käyttäminen. Verkostoautomaation haavoittuvuuksia on kuvattu taulukoissa 3, 4, 5 [17, 18].

Taulukko 3. Haavoittuvuudet verkostoautomaation alustan rakenteessa [17].

Haavoittuvuus	Kuvaus
Varus- ja sovellusohjelmistojen korjauspäivitykset puutteellisia	Automaatiojärjestelmiin tehtävät ohjelmistokorjaukset ja päivitykset ovat työläitä ja vaativat perusteellista testausta ennen tuotantoympäristöön asentamista. Tämä mahdollistaa haittaohjelmille laajan aikaikkunan tehdä hyökkäyksiä
Varus- ja sovellusohjelmistot vanhentuneita ja poistuneet ylläpidon piiristä	Ohjelmistot voivat olla niin iäkkäitä, että niitä ei enää ylläpidetä eikä korjauspäivityksiä ole saatavana, vaikka uusia haavoittuvuuksia löydettäisiin
Järjestelmän käyttöönotto ilman perusteellista testausta	Järjestelmän testaus voi olla puutteellista niin toimittajan kuin tilaajankin puolelta. Varsinkin tietojärjestelmissä voi olla paljon puutteita ja virheitä käytön alkaessa. Nämä voivat sisältää hyvin moninaisia uhkia tietoturvalle
Ohjelmistojen päivityksiä on toteutettu puutteellisin testauksin	Tietoturvapäivitysten puutteellisista testauksista johtuen järjestelmässä voi esiintyä toimintahäiriöitä tai se voi kaatua kokonaan. Ohjelmistopäivitysten ohjeistus tulisi laatia ja dokumentoida
Käytetään oletusparametrointia	Oletusparametrien käyttäminen varus- ja tietoliikenneohjelmistoissa jättää auki olevia tietoliikenneportteja sekä mahdollistaa haitallisten sovellusten ajamisen palvelimissa ja työasemissa
Kriittisistä järjestelmä-konfiguraatioista ja –parametreista ei ole varmuuskopioita	Järjestelmän haavoittuessa, kaatuessa tai toimiessa muutoin puutteellisesti järjestelmä palautetaan puutteellisilla tai vanhentuneilla asetuksilla ja tietomalleilla. Järjestelmä ei toimi oikein
Suojaamattomat kannettavat laiteet ja massamuistit	Luottamuksellinen aineisto tai muutoin sensitiivinen data voi joutua sopimattomalle taholle, mikäli niitä säilytetään huolimattomasti esimerkiksi salaamattomilla laitteilla tai muistivälineillä
Salasanat eivät ole käytössä	Verkostoautomaatiojärjestelmien osajärjestelmät ja työasemat tulee olla varustettu pääsyn ja käyttöoikeuksien hallinnalla asiattoman käytön estämiseksi
Salasanan paljastuminen	Salasanojen huolimattoman säilytyksen tai muun käsittelyn takia ne päätyvät asiattomiin käsiin aiheuttaen hyökkäysriskin
Salasanan riittämätön vahvuus	Hyökkääjä murtaa liian lyhyet, yksinkertaiset tai muutoin helposti johdettavat salasanat

Taulukko 4. Haavoittuvuudet verkostoautomaation fyysisessä osassa [17].

Uhka / Haavoittuvuus	Kuvaus
Järjestelmälaitteiden riittämätön fyysinen suojaus	Valvomo- ja laitetilojen sekä sähköasemien fyysinen suojaus ja kulunvalvonta ovat riittämättömiä, mikä voi mahdollistaa asiattoman pääsyn laitetiloihin ja laitteisiin. Miehittämättömillä asemilla ei ole sähköistä video- tms. valvontaa. Riski laajalle kirjolle erilaisia haitallisia toimenpiteitä sekä uhka luonnononnettomuuksien ja poikkeuksellisten sääilmiöiden aiheuttamille vaurioille
Turvattomat ulkoiset yhteydet	Verkostoautomaatiojärjestelmien tietoverkkoon tulevat, huonosti suojatut ulkoiset yhteydet mahdollistavat asiattoman pääsyn laitteisiin/järjestelmiin. Palomuurit, DMZ-alueen välityspalvelimet etäkäytön RAS-palvelimet tms. ja IDS/IPS-järjestelmät ovat välttämättömiä turvallisen tietoverkon yhdysliikennekäytävissä. Suorat yhteydet julkiseen verkkoon automaatioverkosta eivät ole suositeltavia. Jos niitä on rakennettava pakottavista syistä, on niissä käytettävä lisäksi vahvaa salausta ja käyttäjien vahvaa autentikointia
Runsaasti järjestelmäliitäntöjä	Suuri määrä järjestelmistä lähteviä liityntöjä muihin järjestelmiin vaikeuttaa dataliikenteen hallinnointia ja se voi mahdollistaa asiattoman tiedonvälityksen järjestelmästä tai tietoverkosta toiseen
Dokumentoimattomat laite- ja ohjelmistokokoonpanot	Puutteellisesti dokumentoidut laite- ja ohjelmistokokoonpanot mahdollistavat asiattomien osien liittämisen järjestelmään sekä vaikeuttavat palauttamistoimenpiteitä kriisitilanteissa
EMC-häiriöt ja EMP-suojaus	Puutteellinen suojaus sähkömagneettisilta häiriöiltä voi aiheuttaa laitteiden toimintahäiriöitä ja virhetoimintoja erityisesti sähköasemilla kytkentätilanteissa ja ylivirtojen tai ylijännitteiden esiintyessä (esimerkiksi salamointi). Puutteellinen EMP-suojaus (Elektromagneettinen pulssi) altistaa elektroniset laiteet sähkömagneettiselle pulssille elektronisessa sodankäynnissä, seurauksena laitteiden tuhoutuminen
Varmentamaton tehonsyöttö	Kriittisten laitteiden varmentamaton tehonsyöttö tai riittämätön varakäyntiaika voi johtaa järjestelmän kaatumiseen tehonsyötön vikatilanteessa. Jotkin laitteet saattavat parametroitua virheellisesti tehonsyötön palauduttua tai laitteen elektroniset komponentit saattavat vioittua katkoksen yhteydessä
Puutteellinen ilmastointi ja kosteuden säätö	Elektroniset laiteet vanhenevat ja vikaantuvat ennen aikaisesti liian kuumassa ja/tai kosteassa käyttöympäristössä. Modernit prosessoripohjaiset laitteet voivat suojatoimenpiteenä sammuttaa itsensä tai siirtyä alennetun suorituskyvyn tilaan
Varmennusten puuttuminen	Kriittisten laitteiden tai tietoliikenneyhteyksien varmennusten puuttuminen voi johtaa järjestelmän toimimattomuuteen vikatilanteessa

Taulukko 5. Haavoittuvuudet verkostoautomaation sovellusohjelmistossa [17].

Uhka / Haavoittuvuus	Kuvaus
Puskurin ylivuoto	Ohjelmistoissa voi olla puskureiden ylivuotohaavoittuvuuksia, joita hyökkääjät voivat hyödyntää, mikäli ne ovat tiedossa
Ohjelmistojen turvaominaisuudet eivät ole oletusarvoisesti päällä	Turvaominaisuudet voivat olla oletusarvoisesti pois päältä tai ne on voitu sulkea, kaikki tietoliikenneportit auki jne. Turvaominaisuuksista ei ole hyötyä, mikäli ne eivät ole käytössä
Palvelunestohyökkäykset (DoS)	Huonosti suojattuun verkostoautomaatiojärjestelmään voi kohdistua järjestelmäresursseja voimakkaasti kuormittava hyökkäys, joka estää tai hidastaa normaalia palvelutuotantoa. Tämä ei ole ongelma asianmukaisesti rakennetussa järjestelmäarkkitehtuurissa oleville verkostoautomaatiojärjestelmille, mutta hyökkäys voi kaataa esimerkiksi verkkoyhtiön nettisivut
Tietopakettien virheellinen käsittely	Joissain verkostoautomaatiojärjestelmissä voi esiintyä virhetoimintoja, mikäli ne vastaanottavat korruptoituneita tai tahallisesti virheellisenä lähetettyjä tietopaketteja sisältäen esimerkiksi ei sallittuja muuttujien arvoja
Turvattomien tietoliikenne-protokollien käyttäminen	Käytönvalvontajärjestelmissä yleisesti käytetyt protokollat (esimerkiksi IEC 60870-5-101 ja -104, DNP3 vanhemmat versiot ja Modbus) eivät rakenteellisesti sisällä tietoturvaominaisuuksia ja ovat siten hyvin haavoittuvia
Tarpeettomien prosessien ajaminen	Monissa yleisiä käyttöjärjestelmiä käyttävissä verkosto-automaatiojärjestelmissä tietoliikennepalvelut ovat päällä oletusarvoisesti ja aiheuttavat haavoittuvuusriskin
Avoimesti saatava järjestelmätietous	Yleisimpien järjestelmien järjestelmäspesifikaatiot ja ylläpitokäsikirjat ovat julkisesti saatavissa ja helpottavat hyökkäysten suunnittelua
Järjestelmävalvojan käyttöoikeuksien huolimaton hallinta ja käsittely	Järjestelmävalvojan ja –ylläpitäjän käyttöoikeuksien päätyminen asiattomiin käsiin altistaa järjestelmän väärinkäytöksille ja hyökkäyksille
IDS/IPS-hyökkäyksen-estojärjestelmää ei käytetä	Palomuurien lisäksi IDS/IPS-järjestelmät ovat tehokas keino suojata verkostoautomaatiojärjestelmien tietoverkkoja ei toivotulta liikenteeltä
Lokeja ei hyödynnetä tai seurata reaaliaikaisesti	Ilman ajantasaisia ja tarkkoja lokitietoja ei usein ole mahdollista selvittää tietoturvapoikkeaman aiheuttajaa. Sama koskee muita turvallisuusindikaattoreita
Virustorjunta- ja muita suojausohjelmistoja ei ole käytössä	Monet verkostoautomaatiojärjestelmät eivät toimi virheettömästi, mikäli virustorjuntaohjelmia otetaan käyttöön. Tästä aiheutuu merkittävä riski haittaohjelmien tunnistamiselle ja eristämiselle

Tietoliikenteen haavoittuvuus voidaan jakaa fyysiseen haavoittuvuuteen ja konfiguraation haavoittuvuuteen. Fyysistä haavoittuvuutta kuvaa esimerkiksi huonosti suojatut ulkoiset yhteydet ja konfiguraatio haavoittuvuutta laitteiden oletusparametrien käyttäminen. Tietoliikenteen haavoittuvuuksia on kuvattu taulukoissa 6 ja 7 [17, 18].

Taulukko 6. Haavoittuvuudet tietoliikenteen fyysisessä osassa [17].

Haavoittuvuus	Kuvaus
Turvaton tietoliikeverkon rakenne ja siirtomedia	Tietoliikenneverkon rakenne on suunniteltu yleistä yritysteletoimintaa varten, eikä siinä ole huomioitu toimintakriittisten verkostoautomaatiojärjestelmien tietoliikenteen erityisiä turvallisuus-, luotettavuus ja laitevaatimuksia. Esimerkiksi valokaapeleiden avulla toteutetut siirtomediat ovat yleensä luotettavampia ja tietoturvallisempia kuin langattomat yhteydet
Tietoliikenneverkon ja sen laitteiden riittämätön fyysinen suojaus, esimerkiksi laitetilojen suojausluokitus ei ole riittävä, kuluvalvonta tai lukitus puutteellisia tai laitteita ei ole sijoitettu lukittuihin laitekaappeihin. Laitteiden portit ja liitännät fyysisesti ja loogisesti suojaamattomia	Telelaitetilojen, sähköasemien ja telelaitteiden riittämätön tai puuttuva fyysinen suojaus ja kulunvalvonta voi mahdollistaa huomaamattoman tunkeutumisen laitetiloihin ja laitteisiin. Miehittämättömillä asemilla ei ole esimerkiksi etävideo- tai sähköistä kulunvalvontaa. Riski kohdistuu laajalle kirjolle erilaisia haitallisia ja vihamielisiä toimenpiteitä. Uhka luonnononnettomuuksien ja poikkeuksellisten sääilmiöiden aiheuttamille vaurioille
Tietoliikenneyhteydet ovat varmentamattomia	Verkostoautomaatioyhteyksiltä edellytetään yleensä hyvin korkeaa käytettävyyttä, mikä vaati yhteyksien riippumatonta reitti- ja laitevarmennusta (esim. kahdennus). Myös tehonsyötöt ja kriittisten laitetilojen ilmastointijärjestelmät tulee kahdentaa tai niiden toimintaa tulee valvoa reaaliaikaisesti
Ulkoiset yhteydet ovat huonosti suojattuja	Ulkoiset yhteydet salaamattomia; ei käytetä VPN-tunnelointia tai vahvaa autentikointia
Puutteellinen tai tarkkuudeltaan riittämätön tietoliikenneverkon synkronointi	Puutteellisesti toimiva synkronointi voi aiheuttaa tiedonsiirtovirheitä tai kaataa tietoliikenneverkon tai sen solmuja erityisesti piirikytkentäisissä tietoliikenneverkoissa (esim. SDH- tai PDH-verkot). Myös paketti-kytkentäisissä verkoissa (mm. IP-verkot) synkronointi ja aikaleimojen siirto on toteutettava luotettavasti verkostoautomaatiojärjestelmän asettamien vaatimusten mukaisesti
Palomuureja, välityspalvelimia (proxy) tai IDS/IPS-järjestelmiä ei käytetä	Palomuurit sekä välityspalvelimet ja IDS/IPS- järjestelmät ovat oleellinen osa tietoliikenteen suojausta ja mahdollistavat liikenteen rajoittamisen sekä DMZ-alueiden rakentamisen
Tietoliikenneverkon salaus- ja suojausominaisuudet (laitteet ja ohjelmistot) puuttuvat kokonaan tai ovat puutteellisia	Tietoliikenneverkko ei mahdollista liikenteen salausta tai VPN-tunnelontia, jolloin turvallisuuskriittinen data, esimerkiksi salasanat, voivat joutua asiattomien käsiin

Taulukko 7. Haavoittuvuudet tietoliikenteen konfiguraatiossa [17].

Haavoittuvuus	Kuvaus
Puutteellinen tietoliikenteen reititys- ja access-parametrien hallinta sekä monimutkainen tai sekava verkkorakenne	Puutteellinen tietoliikenneverkon liikenteen hallinta mahdollistaa ei toivottujen järjestelmien/laitteiden kytkeytymisen verkostoautomaatiojärjestelmän laitteisiin, esim. puutteellisesti määritellyt palomuurisäännöt. Rakenteellisesti monimutkaisessa tai sekavassa verkossa ei aina hallita kaikkia tietoliikenteen mahdollisia reittejä
Laitteiden oletusparametrien käyttäminen	Asiattomat tahot pääsevät tunkeutumaan helposti tietoliikenneverkkoon tai sen laitteisiin käytettäessä käyttöoikeuksiin tai porttien aktivointiin yms. liittyvien tunnusten tai parametrien oletusarvoja
Tietoliikenneverkon konfiguraatioparametrien varmuuskopioinnin puuttuminen tai puutteet	Puuttuvat tai puutteelliset (esim. vanhentuneet) laite- ja järjestelmäparametrien varmuuskopiot voivat estää tietoliikenneverkon tai sen osan palauttamisen kriisitilanteessa
Tietoliikenneverkolla ei ole hallintajärjestelmää tai se on rakenteeltaan ja ominaisuuksiltaan puutteellinen	Tietoliikenneverkon hallintajärjestelmä mahdollistaa verkon keskitetyn ja reaaliaikaisen vikojen paikannuksen, verkon konfiguroinnin, siirronlaadun ja turvallisuus-parametrien seurannan sekä hallinnan
Tietoliikenneverkon hallintajärjestelmä tai verkon laitteiden hallintaliittymien käyttöoikeuksien riittämätön tai puuttuva hallinta	Tietoliikenneverkon hallintajärjestelmien tai –liittymien puutteellinen hallinta mahdollista asiattomien henkilöiden tai järjestelmien pääsyn tietoliikenneverkkoon ja voi johtaa tietoliikenneverkon rikolliseen haltuunottoon. Käyttöoikeuksiin liittyviä tunnuksia ja salasanoja ei vaihdeta säännöllisesti tai niiden rakenne on liian yksinkertainen
Hallintajärjestelmän ja/tai verkkolaitteiden lokeja ei hyödynnetä tai seurata systemaattisesti	Ilman ajantasaisia ja tarkkoja lokitietoja ei usein ole mahdollista selvittää laitteiden luvatonta käyttöä tai tietoturvapoikkeaman aiheuttajaa. Sama koskee muita turvallisuusindikaattoreita
Automaatiojärjestelmien vaatimaa turvallista verkkoa ei ole määritelty tai rajattu	Turvallisen verkon määrittely ja dokumentointi on edellytys verkon tehokkaalle suojaukselle
Turvallisessa verkossa siirretään turvatonta tai väärää liikennettä	Turvallista verkkoa käytetään myös muiden kuin verkostoautomaatiojärjestelmien tiedonsiirtoon, josta aiheutuu teknisiä ja turvallisuusriskejä
Avoimesti saatava järjestelmätietous	Suosittujen verkkolaitteiden rakennedata ja ylläpitokäsikirjat ovat julkisesti saatavissa ja helpottavat hyökkäysten suunnittelua

5.5 Suomen automaatioverkon haavoittuvuus

Aalto- yliopiston Sähkötekniikan korkeakoulun Tieliikenne- ja tietoverkkotekniikan laitos tutki tammi- maaliskuun aikana v. 2013 Suomen automaatioverkkojen haavoittuvuutta ja laati raportin, jonka mukaan suojaamattomia tehdasautomaatiolaitteita löytyi verkosta yhteensä 2915 kappaletta. Tästä määrästä 77 olivat sellaisia, joita todennäköisesti käytetään teollisuuden kriittisissä järjestelmissä ja edelleen 33 sellaista, jotka viittaavat suoraan SCADA- järjestelmään. Osa näistä laitteista kuului sähkönhallintaan ja järjestelmien etäkäyttöön, jotka ovat erityisen haavoittuvia Internetistä tulevia kyberhyökkäyksiä vastaan[34].

Avoimia ja suojaamattomia SCADA- ja tehdasautomaatiojärjestelmiä kartoitettiin Shodan- nimisellä hakupalvelulla, jonka toiminta perustuu satunnaiseen porttiskannaukseen. Tutkimuksessa käytettiin tiettyjä hakusanoja, IP- osoiterajauksia sekä protokollia, jotka luovutettiin ainoastaan viranomaiskäyttöön. Shodanin saamien vastausten avulla kyetään selvittämään muun muassa käytettävät ohjelmistoversiot sekä mahdollinen autentikoinnin tarve [34].

Tietoturvan kannalta hälyttävintä tutkimuksen mukaan oli se, että verkosta löytyi paljon sellaisia laitteita, joiden ei tulisi olla julkisesti näkyvillä. Hyökkäysrajapintoina käytetään etäkäyttöliittymiä, palomuureja ja reittimiä, VPN:t sekä haavoittuvat liikennöinti protokollat. Tutkimuksessa löydettiin kahdeksan kappaletta Siemens Simatic S7 PLC- laitteita, jotka olivat yleisesti käytössä Iranin ydinvoimaloissa ja joissa Stuxnet- verkkomato aiheutti huomattavaa vahinkoa. Lisäksi tutkimuksessa raportoidaan kahdeksasta Pocket CMD- käyttöliittymästä, jotka eivät vaatineet minkäänlaista salasanaa ja joita kyettiin ohjaamaan suoraan komentoriviltä. Kuvassa 10. on esitetty kontrollijärjestelmäkomponenttien sijaintia automaatioympäristössä [34].

Kuva 10. Kontrollijärjestelmäkomponentit [34].

Edellä olevan kaltaisiin järjestelmiin pääsy voi mahdollistaa suurenkin katastrofin ainekset ja ne ovat tästä syystä erityisen herkkiä, kyberturvallisuutta ajatellen [34].

Tutkimuksen mukaan, avoimia automaatiolaitteita löytyy jatkuvasti lisää. Kahden viime vuoden aikana kasvuvauhti pelkästään Suomessa on ollut 200 % per vuosi. Tämä on huolestuttavaa sillä turvallisuudesta vastaavat tahot eivät todennäköisesti ole edes tietoisia järjestelmiensä näkyvyydestä Internetissä[34].

Tutkimusraportin lopussa todetaan, ettei Shodanin tietokanta sisällä kokonaisvaltaista otosta Suomen IP- avaruudesta mutta antaa kuitenkin hyvän arvion Suomen tilanteesta automaatiolaitteiden osalta. On luonnollista, että osa kohteista on julkisesti näkyvillä verkossa ja niiden tietoturva on kunnossa mutta että kaikki löydetyt kohteet olisivat tarkoituksellisesti esillä, on vaikea uskoa [34].

6. Tietoturvauhat ja haitat

Tässä luvussa keskitytään teollisuuden automaatiojärjestelmien kannalta haitallisiin haittaohjelmiin ja niiden toimintatapoihin. Käsitellään automaatiojärjestelmälle tärkeitä tietoturvaratkaisuja ja -käytäntöjä. Lopuksi tarkastellaan esimerkin valossa kolmea laajalti julkisuudessa ollutta Stuxnet-, Slammer- ja Sasser- verkkomatoa, jotka kykenivät pysäyttämään teollisuuden automaatiojärjestelmät kokonaan.

6.1. Haittaohjelmat

Haittaohjelma on yleisnimitys erilaisille tietokoneviruksille, roskaposteille, vakoiluohjelmille, rootkiteille, troijalaisille ja verkkomadoille, joiden tarkoituksena on ensisijaisesti aiheuttaa ongelmia ja häiriöitä tietokoneohjelmissa. Haittaohjelmien eri nimitykset johtuvat niiden leviämis- ja toimintatavoista. Jotkut kykenevät leviämään vertaisverkkojen kautta, toisten hyödyntäessä muistitikkuja. Haittaohjelmat voidaan lisäksi luokitella tahallisiksi tai tahattomiksi haittakoodeiksi. Jälkimmäiset eroavat siinä, ettei niiden luomisessa ole ollut kyse tarkoitustahallisuudesta vaan enemmänkin tietämättömyydestä [19].

Rootkit on uudenlainen piilohaittaohjelma, joka kykenee tekemään itsensä täysin huomaamattomaksi, jopa virustorjuntaohjelmilta [19]. Rootkitin kaltaista ohjelmaa hyödynnettiin mm. Stuxnet- verkkomadossa, jossa se vääristi teollisuusprosessin mittausarvoja todellisuudesta siten, ettei itse valvontajärjestelmä osannut reagoida siihen hälytyksellä tai järjestelmän pysäytyksellä vaan ymmärsi prosessin olevan vakaa. Troijan hevonen on yleishyödylliseksi ohjelmakoodiksi naamioitu, joka tosiasiassa sisältää haitallisen toiminnon. Toiminto aktivoituu vasta tietyn ehdon toteutuessa [20].

Haittaohjelmat leviävät useimmiten ohjelmatiedostojen mukana. Tällaisia ohjelmatiedostoja ovat mm. .EXE, .BAT, .COM, .SCR, .PIF ja .ZIP- pääteiset tiedostot. Toinen haittaohjelmien leviämistapa on hyödyntää ns. DLL- tiedostoa. Tämä dynaamisesti ladattava kirjasto on käytössä yleisesti monissa Windows- sovelluksissa [21].

Siirrettävät mediat luovat lisäksi merkittävän uhan haittaohjelmien leviämiselle. USB-muistitikut ja CD/ DVD- levyt ovat erityisen ongelmallisia, erityisesti silloin kun niiden sisältämää tietoa ei ole salattu. Tällaisessa salaamattomassa tiedonsiirtovälineestä haittaohjelma kykenee leviämään nopeasti ja saastuttamaan koneen.

Ohjelmoinnissa tapahtunut tahaton virhe aiheuttaa puskuriylivuodon, jonka avulla hyökkääjä pääsee muokkaamaan ohjelmakoodia järjestelmässä tai kykenee ottamaan haltuunsa koko järjestelmän. Palvelunestohyökkäykset saadaan aikaan niin ikään puskuriylivuodon kautta [22].

6.2 Häivetekniikka

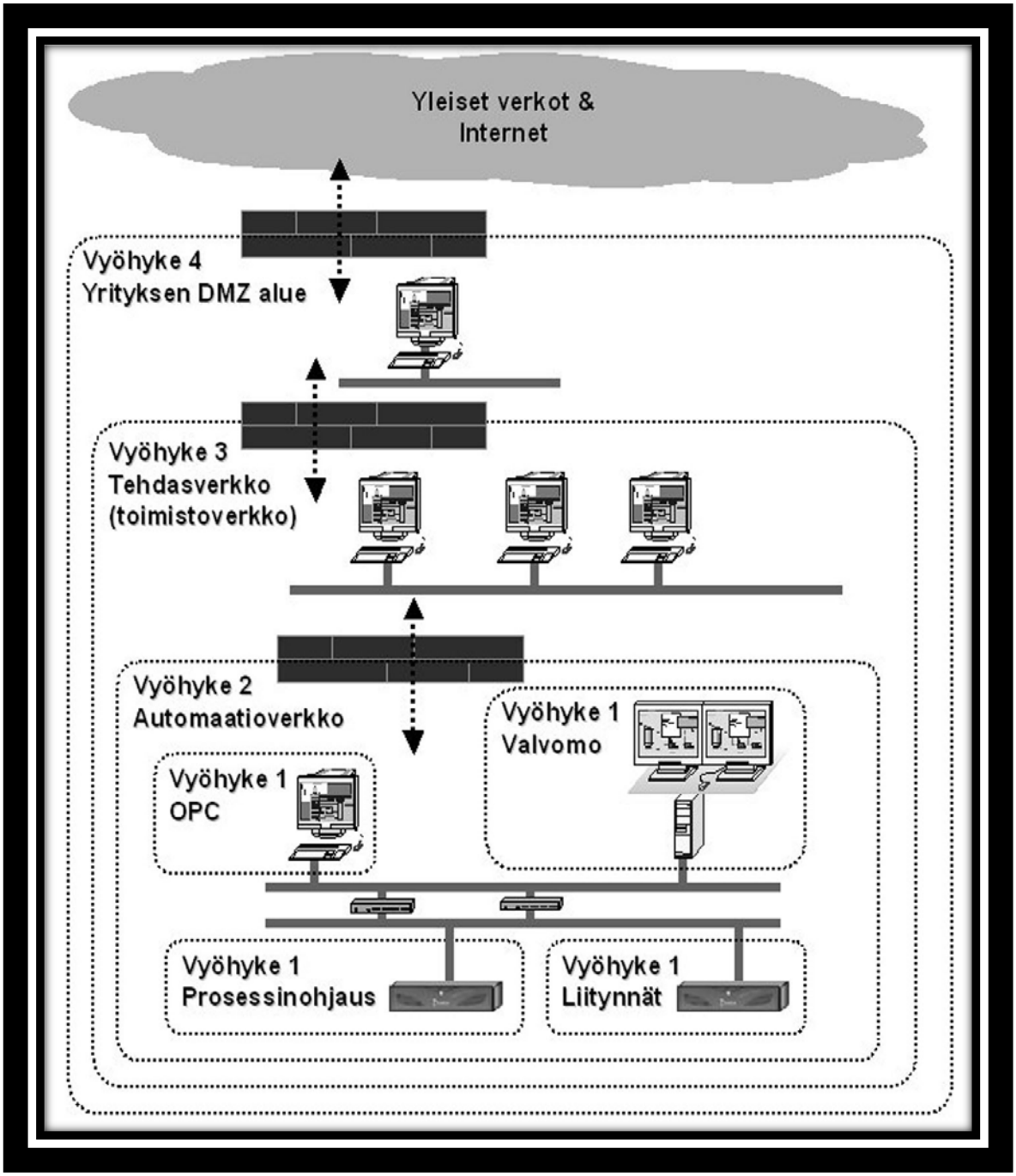
Uudenlaiset häivetekniikat eli evaasiotekniikat ovat tietoturvasta vastaavien ihmisten tämän hetkinen suurin huolenaihe. Kyse on melko uudesta tavasta tarjota verkkorikollisille pääsy haavoittuviin järjestelmiin. Nimensä mukaisesti evaasiotekniikka hyödyntää näkymättömyyttään ja kykenee asentamaan kohteeseen vakoiluohjelman virustorjunnasta ja muista suojausjärjestelmistä piittaamatta. Evaasiotekniikan vaarallisuus piilee sen kyvyssä toimia koko TCP/ IP-protokollapinossa, jossa koko verkkouniversumi toimii. Lisäksi yhdistelemällä ja muuntamalla erilaisia evaasioita, saadaan aikaan se, etteivät palomuurit ja tunkeutumisen estojärjestelmät (IPS) kykene estämään hyökkäyksiä tauottomasta päivityksestä huolimatta [23].

6.3 Automaatiojärjestelmän tietoturva

Perushaaste teollisuusautomaation tietoturvalle on sen jatkuva päivityksen tarve ja tietoturvauhkien muutokset. Automaatiojärjestelmien tietoturvalle on asetettu tietynlaisia perusperiaatteita, joiden mukaan niiden käytössä olevat verkot on erotettu Internetistä palomuureilla ja lisäksi niissä tapahtuva liikenne on tarkoin rajattua. Virustorjuntaohjelmistojen tulee olla ajantasaisia ja kaikkea sähköposti- ja selainliikennettä on tarkkailtava jatkuvasti.[1].

Automaatiojärjestelmien käytettävyyden turvaamiseksi, kaikkien tietoturvaratkaisujen tulee olla asianmukaisesti suunniteltuja, toteutettuja ja ylläpidettyjä.

Yleisesti käytetty suojauskeino teollisuuden automaatiojärjestelmissä on ns. syvyyssuuntainen suojaus, jota on havainnollistettu kuvassa 10. Sen toiminta jakaantuu neljään eri vyöhykkeeseen, joista jokaisella vyöhykkeellä on oma tietoturvatoimenpide. Suojausmenetelmien ei tarvitse olla puhtaasti teknisiä ratkaisuja vaan niihin voidaan sisällyttää esim. tietoturvakoulutusta.[1].



Kuva 10. Automaatioverkon syvyyssuuntainen suojaus. [1]

Koventaminen (hardening) on melko yleisesti käytössä oleva keino ylläpitää automaatiojärjestelmän tietoturvaa. Koventamisella tarkoitetaan sellaista tietoturvatoimenpidettä, jossa automaatiojärjestelmästä poistetaan epäolennaisia ohjelmistoja, palveluja tai muita osuuksia, joille ei löydy tarvetta.

Koventaminen on mahdollista lähes kaikissa järjestelmän osissa ja sitä käytetään erityisesti PC- työasemien ja palvelimien kohdalla. Automaatiojärjestelmän toimivuuden kannalta tarpeettomat käyttöjärjestelmäpalvelut ja liikennöintiraportit voidaan myös poistaa. Suurin huolenaihe on MS Windows- käyttöjärjestelmä, jonka perusoletusarvot sisältävät paljon normaalikäytössä tarpeetonta tietoa. Edellisen lisäksi, automaatioverkko on hyvin yleisesti koventamisen kohteena. Tällä toimella pyritään verkon rajapinnan liikenteen rajoittamiseen[1].

Erittäin tärkeä tietoturvatoimenpide automaatiojärjestelmille on luoda käytänteet liikuteltaville tallennusvälineille. Erityisesti USB- muistit ovat laajalti käytettyjä, ja niiden mukana tuomat riskit on osattava ennakoida ja tiedostaa. Automaattiset käynnistykset tulisi ehdottomasti kyetä estämään automaatioverkon työasemissa[1]. Koventamisesta saatavan hyödyn maksimoimiseksi tulisi ottaa huomioon seuraavat kolme seikkaa:

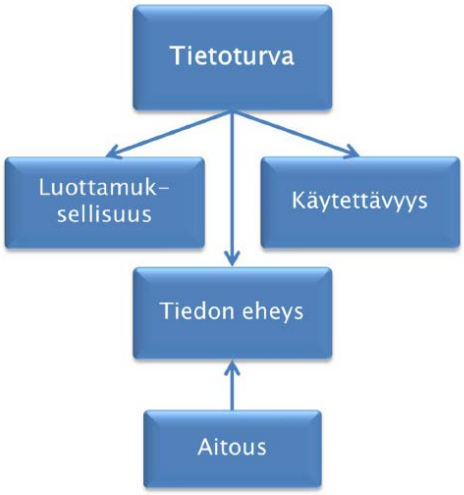
1. Automaatiojärjestelmän koventaminen tulisi tehdä ennen järjestelmän kytkemistä verkkoon.

2. Peruskonfiguroinnissa käyttäjällä ja laitteella tulisi olla vain välttämättömät oikeudet.

3. Koventaminen ei saa häiritä muiden ohjelmien toimintaa.

6.3.1 Avoin lähdekoodi ja tietoturva

Tietoturvalla pyritään estämään tiedon tuhoutuminen, leviäminen väärille tahoille sekä asiasisällön muutokset. Tietoturvaa arvioidaan yleensä kuvan 11. mukaisella jaottelulla.



Kuva 11. Tietoturvan jaottelua [24].

Tiedon luottamuksellisuudella pyritään siihen, että tieto on yksistään tietoon oikeutettujen ihmisten käytössä. Eheydellä huolehditaan sitä, että tiedon sisältöä ei ole luvattomasti muutettu tai, että se olisi virheiden vuoksi muuttunut. Käytettävyydellä tarkoitetaan sitä, että tieto on oikeutettujen käyttäjien saatavilla heti kun sitä tarvitaan. Tiedon aitous voidaan varmentaa sähköisin allekirjoituksin tai digitaalisin varmentein.

Teollisuusautomaation tietojärjestelmissä on yleisesti käytössä laitevalmistajien omia ohjelmistoja, jotka ovat niin sanottuja suljetun koodin ohjelmistoja, joihin ulkopuolisilta pääsy on estetty. Avoimessa järjestelmässä lähdekoodi on kaikkien saatavilla, mahdollistaen ohjelman yksityiskohtaisen tarkastelun ja ohjelmamuutosten tekemisen. Kummassakin järjestelmässä esiintyy riskialttiita sovelluksia mutta onko avoin järjestelmä sittenkin turvallisempi?

Avoimen lähdekoodin sovellukset tarjoavat käyttäjilleen mahdollisuuden analysoida tietoturvaa kooditasolla kun taas suljetussa ohjelmistossa luottamus perustuu laitteen toimittajaan. On osoitettu, että avoimeen lähdekoodiin turvautuvat saavat tietoturvaongelmiinsa ratkaisun huomattavasti nopeammin kuin suljetun koodin käyttäjät. Lisäksi on osoitettu eri tutkimusten yhteydessä, että avoimeen lähdekoodiin tahallisesti ohjelmoidut haavoittuvuudet löytyvät nopeammin kuin suljetussa lähdekoodissa. Selityksenä tälle on annettu , että avoimen lähdekoodin koodimuutoksia seurataan tarkemmin.

On esitetty väitteitä siitä, että avoimen lähdekoodin ohjelmistot ovat suljetun koodin ohjelmistoja turvallisempia. Asiaa on perusteltu sillä, että avoimen lähdekoodin tekemiseen osallistuu suuri määrä ihmisiä, joihin pienemmillä ohjelmistoyrityksillä ei ole resursseja. Tästä on seurauksena se, että laitetoimittajien tietoturvatestaus jää vähäiseksi.

On yleisesti tiedossa tilanteita, joissa tunnettuja haavoittuvuuksia ei uskalleta korjata koska tietoturvakorjauksen julkistaminen yhteydessä myös mahdollinen hyökkääjä saisi tietää mistä kohdin ohjelma on haavoittuvainen. Korjausten asentaminen saattaa olla pitkäkestoinen prosessi, jonka aikana järjestelmä on haavoittuvainen. Tästä syystä moni järjestelmätoimittaja pitää haavoittuvuudet omana tietonaan ja toivoo niiden pysyvän salassa. Avoimessa lähdekoodissa tällaista ongelmaa ei pääse syntymään. Olennaista kaikessa on, että tietoturva on asianmukaisesti hoidettu ja päivitykset suoritettu ajallaan [24].

6.3.2 Suojautuminen hyökkäyksiltä

Sähköverkkoihin kohdistuvia tietoturvauhkia on monenlaisia. Päivittäisiä hyökkäyksiä tai niiden yrityksiä tapahtuu kymmeniä, joista useimmista meillä ei ole mitään tietoa. Kyse on erittäin arkaluonteisista asioista, jotka halutaan pitää ainoastaan viranomaistiedossa. Suojautumisen tärkeyttä ei liioin voi väheksyä, sillä kyse on maailmanlaajuisesta ilmiöstä.

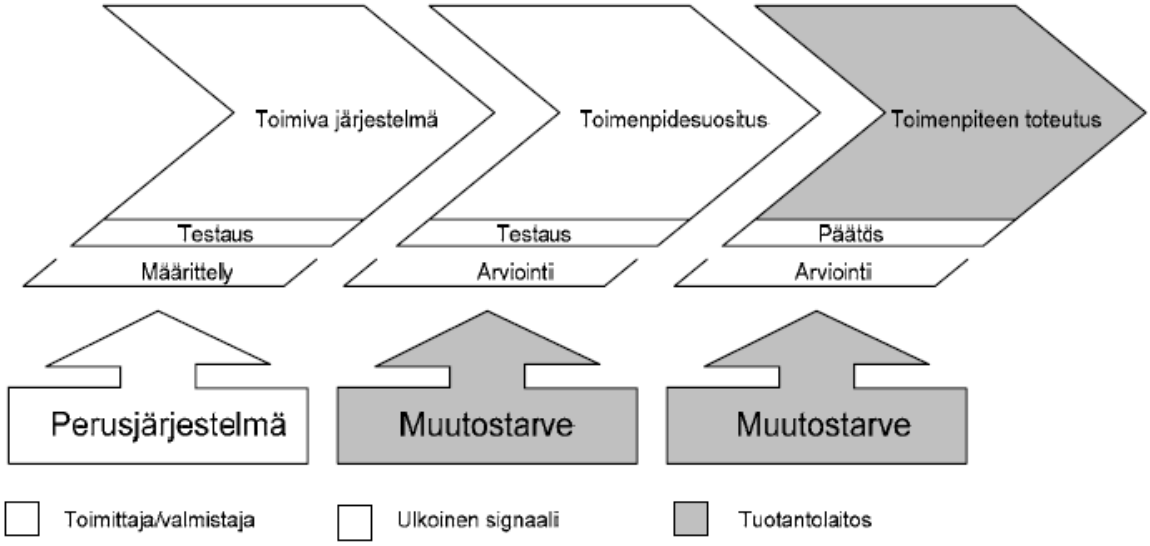
Tietoturvauhat ovat moninaisia ja monelta eri suunnalta leviäviä. Riskianalyysi on yksi tapa selvittää organisaation tietoturvatarvetta, etsimällä järjestelmän heikkouksia ja kehityskohteita.

Suojautumisen edellytyksiä ovat suunnittelu, hyvä järjestelmätuntemus, tekniset tietoturvaratkaisut sekä aika. Edellä mainitut seikat liitettynä tiedon eheyteen, saatavuuteen ja luottamuksellisuuteen takaavat melko hyvän suojautumiskeinon [1].

Useat automaatiojärjestelmien valmistajat luottavat pitkälti omiin tietoturvaperiaatteisiin, joilla saadaan aikaan järjestelmiin sopivat parhaat tietoturvaratkaisut. Automaatiolaitteiden toimittajien ja tilaajien välisen yhteistyön seurauksena on mahdollista aikaansaada tietoturvaan liittyvien toimintaprosessien

yhteensovittaminen ja varmistua siitä, että tuotantolaitoksen tietoturva on korkealla tasolla [1].

Yleiset periaatteet, joilla teollisuuden käytettävyysriskejä voidaan alentaa, ovat ratkaisujen vakiointi, muutosten testaus sekä muutosten toteutus. Yleisiä tietoturvan perusperiaatteita on esitetty kuvassa 12 [1].



Kuva 12. Muutostenhallinnan toimenpiteet [1].

Työasemien suojauksessa automaatioympäristössä tulisi kiinnittää huomiota koventamiseen, käyttöjärjestelmän päivitykseen, virustorjuntaan sekä käyttäjien hallinta- ja salasanakäytäntöön. Kaikki edellä olevat turvaamistoimet tulisi suorittaa seikkaperäisesti, edellyttäen kuitenkin, ettei automaatiojärjestelmän käytettävyys samalla vaarannu. Mikäli laitetta ei saada tietoturvallisemmaksi, tulee se huomioida laitteen käytössä.

Suurin riski käytettävyydessä piilee testaamattomissa ohjelmissa ja tietoturvapäivityksissä. Tämä on paradoksaalista sillä tietoturvapäivitysten laiminlyönti taas lisää käytettävyysriskiä. Perusongelma lienee oikean toimenpiteen löytämisessä siten, ettei käytettävyys kärsi ja tietoturva säilyy [1].

6.3.3 Tunkeutumisen havainnointi- ja estojärjestelmä

Tunkeutumisen havaitsemisjärjestelmän ensisijainen tehtävä on ilmoittaa verkossa tapahtuvat tunkeutumisyritykset. Tämä kyseinen järjestelmä tunnetaan kansanvälisesti nimellä IDS (Intrusion Detection System). IDS- järjestelmän toiminta perustuu oletukseen, jonka mukaan normaali toiminta poikkeaa olennaisesti tunkeilijan toiminnasta [5].

IDS- järjestelmä jakaantuu isäntä- ja verkkopohjaisiin järjestelmiin, jotka voivat toimia joko aktiivisesti tai passiivisesti.

Aktiivisista järjestelmistä käytetään nimitystä tunkeutumisen estojärjestelmä IPS (Intrusion Prevention System) ja passiivisista IDS (Intrusion Detection System). Nämä molemmat ohjelmistot tarkkailevat jatkuvasti mahdollisia väärinkäytöksiä verkosta kerättyjen tilastojen pohjalta tai ennalta määritetyistä säännöistä [5].

Aktiivisella järjestelmällä on kyky reagoida hälytyksiin ja estää haitallinen toiminta yhteyden katkaisulla, kun taas IDS- järjestelmässä haitallisen toiminnan estäminen on ylläpitäjän vastuulla. IDS- järjestelmä ei anna hyökkääjälle minkäänlaista signaalia siitä, että se on tullut havaituksi, vaan jakaa tiedon valvojalle hiljaisena hälytyksenä. Tällä menettelyllä pyritään saamaan lisää tieto tunkeutumistekniikoista ja tunkeilijan motiiveista [5].

IDS- järjestelmä kykenee keräämään systemaattisesti tietoja eri hyökkäystekniikoista, joita hyödynnetään järjestelmän kehityksessä. IDS:n avulla kyetään lisäksi sensoreiden avulla seuraamaan verkkoliikennettä ja käytettäviä protokollia [5].

Tunkeutumisen havaitsemisjärjestelmät toimivat teknisesti samalla tavalla kuin hakkereiden salasanavakoilijat. Tässä piilee tietoturvavaara sillä hakkereiden onnistuessa saamaan haltuunsa IDS- ohjelmiston, kykenevät he urkkimaan salaisia tietoja. Tämän vuoksi IDS- järjestelmä tulee ehdottomasti sijoittaa valvottavan verkon ulkopuolelle [5].

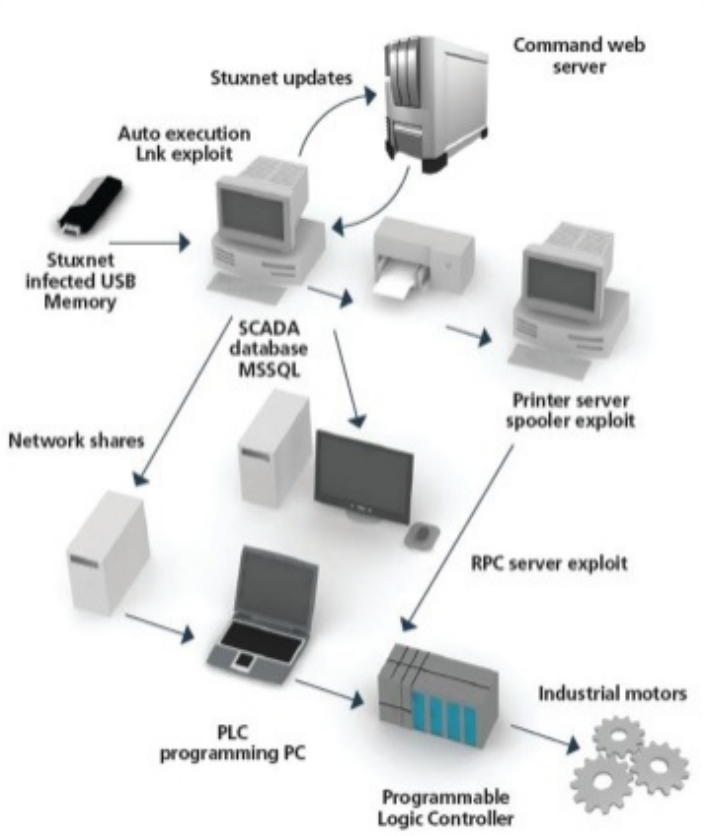
6.4 Stuxnet- verkkomato ja sen toiminta

Stuxnet on maailmanlaajuisesti tunnettu haittaohjelma, eräänlainen täsmäohjattu kyberase, josta tehtiin ensimmäinen havainto kesällä 2010. Sen ensisijaisena kohteena oli teollisuuden valvonta- automaatiojärjestelmä SCADA, johon se saatiin asennettua USB- muistitikun välityksellä. Stuxnet on löytymisensä jälkeen herättänyt suurta mielenkiintoa mediassa ja tietoturvayrityksissä, ei ainoastaan monimutkaisuutensa, vaan sen aikaan saamien vahinkojen vuoksi. Se on ollut merkki uuden kyberaikakauden syntymisestä, jossa toimijoina ovat valtiot ja suuret organisaatiot [16, 25, 26].

Stuxnetin toiminnallisuus perustuu sen kykyyn muuttaa teollisuusautomaatiojärjestelmässä käytetyn ohjelmoitavan logiikkaohjaimen ohjelmakoodia siten, että logiikkaohjaimen toiminta häiriintyy tai estyy kokonaan. Vastaavia PLC (Programmable Logic Controller) logiikkapiirejä on käytössä yleisesti eri automaatioprosessien ohjausjärjestelmissä, joissa niiden tietosuojasta ei ole pidetty riittävää huolta [20].

Stuxnet- mato kykeni hyödyntämään Windows -pohjaisen teollisuusautomaatiojärjestelmän kahta ns. nollapäivähaavoittuvuutta, joista ohjelman kehittäjät eivät olleet tietoisia [27].

Stuxnet- madon kohteena oli Iranin ydinmateriaalin rikastuslaitos ja siellä käytössä olleet Siemensin valmistamat sentrifugien SIMANTIC S7, joiden ohjausjärjestelmää muuttamalla kyettiin hidastamaan Iranin yritystä rikastaa uraania, jopa kahdella vuodella. Tavoitteeseen päästiin kun ohjelman avulla kyettiin antamaan virheellistä arvoja sentrifugien pyörimisnopeudesta vastaaville taajuusmuuttajille. Valvontajärjestelmälle uskoteltiin pyörimistaajuuden säilyneen sallituissa rajoissa. Tosiasiassa sentrifugeja pyörittävät moottorit kävivät ylikierroksilla ja lopulta rikkoivat ne [16, 28]. Haittaohjelman toimintaa havainnollistaa kuva 13 [29].



Kuva 13. Stuxnet- madon leviämistapa [29].

1. Stuxnet- ohjelma leviää järjestelmään USB- muistitikun kautta. Se kykenee saastuttamaan kaikki Windows ohjelmia käyttävät tietokoneet.

2. Stuxnet etsii prosessinohjaukseen käytettäviä Siemens SIMATIC PCS7- ohjelmistoja, joiden avulla ydinlaitoksen sentrifugeja ohjataan.

3. Kohteiden löytymisen jälkeen, haittaohjelma päivittää itsensä verkkoyhteyden kautta.

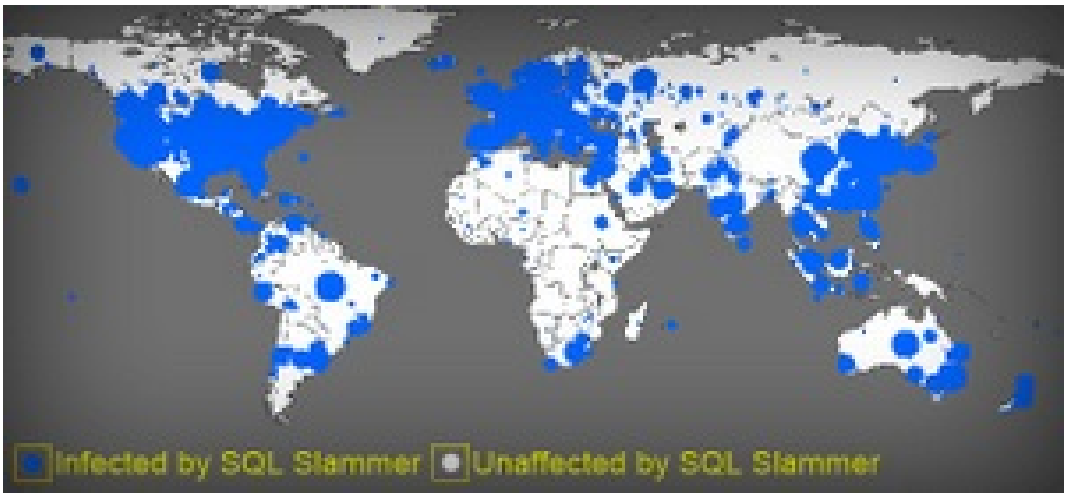
4. Stuxnet selvittää ohjelmoitavien logiikkapiirien nollapäivähaavoittuvuudet ja iskee järjestelmään. Se muuntaa sentrifugeja pyörittävien moottoreiden pyörimisnopeutta.

6.5 Slammer- verkkomato ja sen toiminta

Slammer- niminen verkkomato saastutti Yhdysvalloissa, Ohion osavaltiossa vuonna 2003, ydinvoimalaitoksen ja esti ohjausjärjestelmän toiminnallisuuden neljäksi tunniksi. Tämän lisäksi se kykeni eliminoimaan prosessitietokoneen seitsemäksi tunniksi aiheuttaen tietoverkkojen ja ohjausjärjestelmän ylikuormituksen [30].

Mato pääsi leviämään järjestelmään yhteistyökumppanin tietoverkosta, josta edelleen kaupalliseen tietoverkkoon. Tämän jälkeen mato levisi tietoliikenneyhteyksiä pitkin laajemmalti kriittiseen tietoverkkoon. Yhteys kykeni ohittamaan palomuurin, joka oli asennettu kaupallisen tietoverkon ja kriittisen tietoverkon väliin [30].

Slammer- mato on ollut historiansa nopeimpia verkkomatoja ja sen on laskettu aiheuttaneen kymmenessä minuutissa 750 miljoonan dollarin vahingot. Mato oli ohjelmoitu siten, että se kykeni hyödyntämään Microsoft SQL Serverissä olevaa tunnettua tietoturva- aukkoa. Tämän olemassa olevan aukon avulla se eteni koko Internetin osoiteavaruuteen ja saastutti yli 100 000 tietokonetta. Suurimpia kärsijöitä olivat Yhdysvallat ja Aasia [30]. Slammer- madon saastuttamia alueita on esitetty kuvassa 14 [31].



Kuva 14. Slammer- madon levinneisyys [31].

6.6 Sasser- verkkomato ja sen toiminta

Sasser- mato on kolmas laajalti teollisuusautomaatioon vaikuttaneista haittaohjelmista, joka levisi Internetissä keväällä 2004. Sasser- mato hyödynsi MS Windows-järjestelmässä olevaa LSASS (Local Security Authority Subsystem Service)-haavoittuvuutta [17].

Mato kykeni leviämään toimistoverkkojen kautta suojaamattomiin teollisuusautomaatioverkkoihin. Mato levisi toimistoverkkoihin kannettavien tietokoneiden kautta, joihin se oli tarttunut Internetin välityksellä. Madolla oli muun muassa kyky käynnistää käyttöjärjestelmä uudelleen ja saada aikaan palvelunesto-tilanne [17].

Sasser- madon leviäminen kuormitti verkkoja siten, että liikenne hidastui tai estyi kokonaan. Verkkojen ylikuormittamisesta huolimatta, Sasser ei tuhonnut varsinaisia tiedostoja mutta kykeni aiheuttamaan teollisuusautomaatioympäristössä lukuisia häiriöitä ja alasajoja sekä tuotannon keskeytymisiä. Rahallisen haitan laskeminen on ollut vaikeaa, mutta arvioidaan, että ohjelma kykeni aiheuttamaan yli 400 miljoonan euron kustannukset. Olennaista haittaohjelman leviämisessä oli se, että niissä automaatiojärjestelmissä, joissa tietoturvapäivitykset oli hoidettu asianmukaisesti, ei häiriöitä havaittu [17].

6.7 Rocra- haittaohjelma ja sen toiminta

Rocra- vakoiluverkosto tunnetaan paremmin täällä Suomessa Punaisena lokakuuna, joka on maailmanlaajuinen kybervakoiluhanke, jonka tiedetään saaneen alkunsa jo vuonna 2007. Vakoiluhankkeesta tehtiin ensimmäinen havainto lokakuussa 2012, venäläisen tietoturvayhtiö Kaspersky Lab tutkijoiden toimesta[32].

Red October -vakoiluoperaation saastuttamia järjestelmiä on havaittu myös Suomessa mutta niitä ei ole tuotu julkiseen keskusteluun turvallisuussyihin vedoten. Myös Helsingin rikospoliisi on ottanut tutkittavakseen Rocra- vakoiluverkostosta tehdyn rikosilmoituksen, jonka esitutkinta on vielä kesken [32].

Haittaohjelmahyökkäyksen tarkoituksena on saada haltuun luottamuksellisia asiakirjoja, salasanoja ja käyttäjätunnuksia, geopoliittisesti merkittävää tiedustelutietoa sekä tietoja mobiili- ja verkkolaitteista [32].

Punaisen lokakuun aiheuttamia virustartuntoja on löydetty eniten Saksasta, Venäjältä, Brasiliasta, Australiasta, Yhdysvalloista ja Japanista, joissa niiden kohteiksi ovat joutuneet muun muassa suurlähetystöt ja diplomaattiedustustot, tutkimuslaitokset, ydinvoimalat sekä valtion hallintoelimet. Näiden lisäksi myös ilmakehään ja avaruuteen liittyvät kohteita on joutunut vakoilun alaisiksi, erityisesti Kazakstanin alueella [32].

Hyökkääjät ovat varastaneet haittaohjelman avulla useantyyppisiä tiedostoja kuten: txt, csv, eml, doc, vsd, sxw, odt, docx, rtf, pdf, mdb, xls, wab, rst, xps, iau, cif, key, crt, cer, hse, pgp, gpg, xia, xiu, xis, xio, xig, acidcsa, acidsca, aciddsk, acidpvr, acidppr, acidssa [33].

YHTEENVETO

Työssä tarkasteltiin sähköverkkojen kyberturvallisuutta sähkönsiirto- ja jakeluverkoissa. Tarkastelun kohteena olivat eri sähkönjakelun automaatiotasot, päähuomion kiinnittyessä käytönvalvonta- ja käytöntukijärjestelmään ja niiden komponentteihin sekä liikennöintiprotokolliin. Työssä selvitettiin verkostoautomaatioon kohdistuvia tietoturvauhkia ja haavoittuvuuksia ja niiltä suojautumista. Lisäksi tarkasteltiin viime aikoina julkisuuteen nousseita kansainvälisen huomion saaneita kyberiskuja ja niissä käytettyjä haittaohjelmia.

Käytönvalvontajärjestelmiin kohdistuvat kyberuhat ovat luonteeltaan samanlaisia kuin muissakin tietoverkoissa. Infrastruktuuria vastaan tapahtuvien hyökkäysten määrä on noussut viimeisen parin vuoden aikana rajusti, johon myös Suomen valtio on reagoinut omalla kyberturvallisuusstrategiallaan. Perinteisten hakkereiden ja tietorikollisten lisäksi myös valtiolliset toimijat ovat astuneet sähköiseen kybersodankäyntiin.

Tietoturvauhkia ja -haavoittuvuuksia on verkottumisen myötä yhä enemmän. Syy tähän on tietotekniikan siirtyminen erilaisiin käyttöjärjestelmiin ja ohjelmistoalustoihin. Lisääntynyt älykkäiden laitteiden määrä ja siirtyminen älykkääseen sähköverkkoon on tuonut oman haasteensa verkostoautomaatiojärjestelmien tietoturvalle. Sähköverkkolaitteiden määrän huomattava kasvu ja sovellusten monimutkaistuminen kuin myös etätyöskentelyn yleistyminen Internet- verkon yli on lisännyt paineita tietoturvalle.

Käytönvalvontajärjestelmät ovat sähkönjakelun kannalta kriittisimpiä kohteita kyberiskulle. SCADA- järjestelmän arkkitehtuurisuunnittelulla ja henkilökunnan tietoturvakoulutuksella kyetään pienentämään tämänkaltaisia riskejä. Tunkeutumisen havainnointi- ja estojärjestelmien hyödyntäminen ja huolehtiminen SCADA-järjestelmän ohjelmiston ajanmukaisesta päivittämisestä parantaa huomattavasti koko sähköjärjestelmän kokonaisturvallisuutta.

Viime vuosina koetut kyberiskut ja niissä käytetyt haittaohjelmat kuten Stuxnet, Sasser, Slammer ja Rocra ja ovat osoituksia vakavista infrastruktuuriin kohdistuvista hyökkäyksistä, jotka ovat saaneet suurta tuhoa aikaan.

Tämänkaltaiset haittaohjelmat ovat osoittautuneet pääsääntöisesti valtiollisten toimijoiden kehittämiksi ja joissa intressit ovat maailmanpoliittisia.

SCADA- järjestelmään kohdistuvat kyberturvallisuusuhat muodostuvat edellisen kaltaisista haittaohjelmista, kehittyneistä evaasiotekniikoista sekä huonosta tietoturvapolitiikasta. Palvelunestohyökkäys on kuitenkin todennäköisin uhka nykypäivän sähköverkolle ja huolehtimalla oikeanlaisesta perustietoturvasta, voidaan tämänkaltaiselta ongelmalta välttyä.

LÄHTEET

[1] Teollisuusautomaation tietoturva, Verkottumisen riskit ja niiden hallinta, ISBN 978-952-5183-38-2.

[2] Lakervi, Erkki, Partanen, Jarmo; Sähkönjakelutekniikka; Gaudeamus Helsinki University Press/ Otatieto, Helsinki 2008.

[3] Martikainen, Jari; Käytönvalvontajärjestelmä. Helsinki: Fingrid Oyj:n lehti 1/2005.

[4] Elovaara, Jarmoa ja Haarla, Liisa; Sähköverkot II, Verkon suunnittelu, järjestelmät ja laitteet; Gaudeamus Helsinki University Press/ Otatieto, Helsinki 2011.

[5] Ekman, Jani, Tunkeutumisenesto ja havainnointi käytönvalvontajärjestelmässä, Opinnäytetyö, Metropolia Tietoliikennetekniikka.

[6] Piispanen, Markus Diplomityö; Synenergioiden saavutettavuus automaattisessa mittarinluennassa sähkö-, kaukolämpö- ja vesihuoltoyhtiöiden välillä.

[7] Illinois, IEC 61850 – Communication Networks and Systems in Substations. Saatavissa: http://seclab.uiuc.edu/docs/iec61850-intro.pdf.

[8] OSI-malli.jpg. Saatavissa: http://fi.wikipedia.org/wiki/Tiedosto: (Viitattu 24.10.2013).

[9] Shaw, William T, Cybersecurity for SCADA Systems. Tulsa, Oklahoma: PennWell Corporation. 2006.

[10] Modbus-IDA, Modicon Protocol Reference Guide (verkkodokumentti, Saatavissa: http://modbus.org/docs/PI_MBUS_300.pdf. (Viitattu 6.9.2013)

[11] Jantunen, Matti, Käytönvalvontajärjestelmä SCADA; Ominaisuudet ja käyttö, Seminaarityö, Lappeenrannan teknillinen yliopisto, Lappeenranta, 2003.

[12] Saatavissa: http://energia.fi/sites/default/files/inca_loppuraportti_final.pdf (Viitattu 27.10.2013).

[13] Saatavissa: http://www.ajeco.fi/pdf/DSiP_brochure_v2.2-1.pdf. (Viitattu 27.10.2013).

[14] VTT:n tiedote 2545, 2010, TITAN- käsikirja, Saatavissa: http://www.vtt.fi/inf/pdf/tiedotteet/2010/T2545.pdf. (Viitattu10.10.2013).

[15] Pullinen, Mika- Jan, Opinnäytetyö, Kriittisten tietojärjestelmien suojaaminen kyberuhilta. Saatavissa: http://publications.theseus.fi/bitstream/handle/10024/46341/Pullinen_Mika.pdf?sequence=1 7(Viitattu 7.8.2013).

[16] Suomen kyberturvallisuusstrategia. Saatavissa: http://www.yhteiskunnanturvallisuus.fi/fi/materiaalit?start=5.(Viitattu 23.6.2013).

[17] Tervo, Jouko Verkostoautomaatiojärjestelmien tietoturva 2013, Saatavissa: http://energia.fi/sites/default/files/dokumentit/ajankohtaista/Tapahtumat/2013/ST- pooli/esitys_tervo.pdf (Viitattu 14.10.2013).

[18] NIST (National Institute of Standards and Technology), Special Publication 800-82 guide to Supervisory Control and Data Acquisition (SCADA) and Industrial Control System Security, Revision 1, NIST. Saatavissa:http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf (viitattu: 14.10.2013).

[19] Saatavissa: http://www.tietoturvaopas.fi/uhatjaniidentorjunta/haittaohjelmat.html.

[20] Karnouskos, S, IECON 2011- 37th Annual Conference on IEEE Industrial Electronics Society. Stuxnet Worm Impact on Industrial Cyber- physical System Security. 978-1-61284-972-0/11. IEEE CONFERENCE PUBLICATIONS.

[21] Saatavissa: http://www.cert.fi/tietoturvanyt/2010/08/ttn201008251616.html (Viitattu: 16.10.2013).

[22] Viestintäministeriö. Haavoittuvuudet 2008, verkkodokumentti. Saatavissa http:/www.cert.fi/haavoittuvuudet.html. (Viitattu 27.10.2013).

[23] Saatavissa: http://www.stonesoft.com/en/company/press and media/releases/fi/2011/15022011.html.

[24] Saatavissa: http://www.relator.fi/docs/Tietoturva.pdf (Viitattu: 24.10.2013).

[25] Saatavissa: http://www.cert.fi/katsaukset/2010/tietoturvakatsaus_3_2010.html (Viitattu 18.10.2013).

[26] Sheng, Su; Yingkun, Wang; Yuyi, Long; Yong, Li; Yu, Jiang. Reliability of Transmission and Distribution Networks (RTDN 2011), IET Conference. Cyber attack impact on power system blackout. IET CONFERENCE PUBLICATIONS.

[27] Kriaa, S; Bouissou, M; Pietre- Canbacedes, L. Risk and Security of Internet and Systems (CRiSIS), 2012 7th International Conference. Modeling the Stuxnet Attack with BDMP: Towards More Formal Risk assessments. IEEE CONFERENCE PUBLICATIONS.

[28] Saatavissa: http://www.f-secure.com/weblog/archives/00002066.html (Viitattu: 18.10.2013).

[29] Saatavissa: http://eandt.theiet.org/magazine/2012/09/images/640_stuxnet.jpg.

[30] Saatavissa: http://www.symantec.com/security_response/writeup.jsp?docid=2003-012502-3306-99. (Viitattu 28.10.2013).

[31] Saatavissa: http://listdose.com/wp-content/uploads/2013/08/SQL-Slammer.jpg (Viitattu 28.10.2013).

[32] Saatavissa: http://www.securelist.com/en/analysis/204792262/Red_October_Diplomatic_Cyber_Attacks_Investigation; (Viitattu 23.11.2013).

[33] Saatavissa: http://www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies (Viitattu: 23.11.2013).

[34] Saatavissa: https://research.comnet.aalto.fi/public/Aalto-Shodan-Raportti-julkinen.pdf.(Viitattu 28.11.2013).

LIITE A.

Asiantuntijoiden kanssa käydyt keskustelut

25.02.2013

Kim Malberg

Netcontrol Oy

Tapaamisessa keskusteltiin Suomen kyberturvallisuusosaamisesta ja varautumisesta siihen. Käytiin lyhyesti läpi yhtiön kaupallisia tuotteita.

27.03.2013

Juha Haikonen

Tekla

Keskusteltiin yleisellä tasolla sähkönjakeluautomaatiojärjestelmässä käytettyjen ohjelmistojen tietoturvasta sekä käytiin läpi Teklan kaupallisia tuotteita sähköverkkoteollisuudelle.

02.04.2013

John Holmström

Ajeco Oy

Keskustelun aiheena oli sähköverkkojen tiedonsiirto sekä kyberturvallisuus. Käytiin läpi yhtiön toimintaa ja perehdyttiin yhtiön luomaan DSiP- järjestelmään ja sen toimintaan.

10.05.2013

Jyrki Penttonen

Viola Systems

Tapaamisessa keskusteltiin mm. Yhdysvaltojen, Israelin sekä Viron kyberturvallisuusosaamisesta. Lisäksi pohdittiin Suomen tilannetta ja sitä kuinka huonosti sähköverkkoyhtiöt tosiasiassa tunnistavat omat heikkoutensa tietoturva- asioissa.